G.SHDSL.bis Router

User Manual

Version 0.01

Table of Contents

1 DESCRIPTIONS 5

1.1 FEATURES 5
1.2 SPECIFICATION 6
1.3 APPLICATIONS 9

2 GETTING TO KNOW ABOUT THE ROUTER 10

2.1 FRONT PANEL 10
2.2 REAR PANEL 12
2.3 SHDSL.BIS LINE CONNECTOR 13
2.4 CONSOLE CABLE 13

3 INSTALLING THE ROUTER 14

3.1 CHECK LIST 14
3.2 INSTALL THE SHDSL.BIS ROUTER 16

4 CONFIGURATION VIA WEB BROWSER 18

4.1 BASIC SETUP 22
4.1.1 Bridge Mode 22
4.1.2 Routing Mode 25
4.1.3 Reference diagram 33
4.2 ADVANCED SETUP 35
4.2.1 SHDSL.bis 35
4.2.1.1 Annex Type 36
4.2.1.2 Line Type 36
4.2.1.3 TCPAM Type 38
4.2.1.4 Data Rate 38
4.2.1.5 SNR Margin 38
4.2.1.6 TC Layer 38
4.2.1.7 Line Probe 39
4.2.2 WAN 39
4.2.3 Bridge 41
4.2.4 VLAN 44
4.2.4.1 802.1Q Tag-Based VLAN 45
4.2.4.2 Port-Based VLAN 45
4.2.5 STP 47
4.2.6 Route 49
4.2.7 NAT/DMZ 53
4.2.7.1 Multi-DMZ 54
4.2.7.2 Mutli-NAT 54
4.2.8 Virtual Server 55
4.2.9 Firewall 57
4.2.9.1 Basic Firewall Security 57
4.2.9.2 Automatic Firewall Security 58
4.2.9.3 Advanced Firewall Security 59
4.2.10 IP QoS 63
4.3 STATUS 66

4.3.1 SHDSL.bis *67*
4.3.2 LAN *68*
4.3.3 WAN *69*
4.3.4 ROUTE *70*
4.3.5 INTERFACE *71*
4.3.6 FIREWALL *72*
4.3.7 IP QoS *73*
4.3.8 STP *74*
4.4 ADMINISTRATION 76
4.4.1 Security *76*
4.4.2 SNMP *78*
4.4.2.1 Community pool 79
4.4.2.2 Trap host pool 79
4.4.3 SYSLOG *80*
4.4.4 Time Sync *81*
4.4.4.1 Synchronization with PC 81
4.4.4.2 SNTP v4.0 82
4.5 UTILITY 83
4.5.1 System Info *83*
4.5.2 SYSLOG *84*
4.5.3 Config Tool *85*
4.5.3.1 Load Factory Default 86
4.5.3.2 Restore Configuration 86
4.5.3.3 Backup Configuration 86
4.5.4 Upgrade *87*
4.5.5 Logout *88*
4.5.6 Restart *89*
4.6 EXAMPLE 90
4.6.1 LAN-to-LAN connection with bridge Mode *90*
4.6.1.1 CO side 90
4.6.1.2 CPE Side 91
4.6.2 LAN to LAN connection with routing mode *92*
4.6.2.1 CO Side 92
4.6.2.2 CPE side 93

5 CONFIGURATION VIA SERIAL CONSOLE OR TELNET WITH MANU DRIVEN INTERFACE 96

5.1 INTRODUCTION 96
5.1.1 Serial Console *96*
5.1.2 Telnet *97*
5.1.3 Operation Interface *97*
5.1.4 Window structure *99*
5.1.5 Menu Driven Interface Commands *100*
5.2 MAIN MENU BEFORE ENABLE 100
5.3 ENABLE 101
5.4 STATUS 102
5.4.1 Shdsl.bis *102*
5.4.2 Wan *103*
5.4.3 Route *104*

5.4.4 Interface *104*
5.4.5 firewall *104*
5.4.6 ip_qos *105*
5.4.7 STP *105*
5.4.8 Clear *106*
5.5 SHOW 106
5.5.1 System information *107*
5.5.2 Configuration information *107*
5.5.3 Configuration with Script format *107*
5.6 WRITE 107
5.7 REBOOT 108
5.8 PING 108
5.9 ADMINISTRATION 108
5.9.1 User Profile *109*
5.9.2 Security *110*
5.9.3 SNMP *111*
5.9.4 Community *112*
5.9.4.1 Trap Host 112
5.9.5 Supervisor Password and ID *113*
5.9.6 SNTP *115*
5.10 UTILITY 117
5.10.1 Upgrade *117*
5.10.2 Backup *117*
5.10.3 Restore *118*
5.11 EXIT 118
5.12 SETUP 118
5.12.1 Operation Mode *119*
5.12.2 SHDSL.bis *119*
5.12.2.1 Mode 120
5.12.2.2 Link 120
5.12.2.3 N*64 120
5.12.2.4 Type 120
5.12.2.5 Margin 120
5.12.2.6 Tcpam 121
5.12.2.7 Probe 121
5.12.2.8 TC Layer 121
5.12.2.9 Clear 121
5.12.3 WAN *121*
5.12.3.1 Protocols 122
5.12.3.2 IP Address 122
5.12.3.3 VPI VCI 122
5.12.3.4 Ecapsulation 122
5.12.3.5 VC QoS 122
5.12.3.6 ISP 123
5.12.3.7 IP Type 123
5.12.3.8 List 123
5.12.4 Bridge *123*
5.12.4.1 Gateway 123
5.12.4.2 Static Bridging Table 124

5.12.5 VLAN 125
5.12.5.1 802.11Q VLAN 125
5.12.5.2 Port Based VLAN 127
5.12.6 STP 127
5.12.7 Route 127
5.12.7.1 Static 128
5.12.7.2 Rip 129
5.12.8 LAN 130
5.12.9 IP share 131
5.12.9.1 NAT 131
5.12.9.2 PAT 134
5.12.9.3 DMZ 135
5.12.10 Firewall 136
5.12.10.1 firewall security level 136
5.12.10.2 Packet Filtering 137
5.12.10.3 DoS Protection 138
5.12.11 IP QoS 140
5.12.12 DHCP 141
5.12.12.1 DHCP Server generic 142
5.12.12.2 DHCP Server Fixed Host 142
5.12.12.3 DHCP Relay 143
5.12.13 DNS proxy 143
5.12.14 Host name 144
5.12.15 Default 144

1 Descriptions

The SHDSL.bis (Symmetric High Speed Digital Subscriber Loop) Routers (with ATM/EFM layer) comply with G.991.2(2004) standard optimized for small to medium size business environment. It provides business-class, multi-range from 192Kbps to 5.696Mbps (for 2-wire model) and 384Kbps to 11.392Mbps (for 4-wire model) symmetric payload rates over exiting copper wire. The various pair bonding techniques make it suitable for any types of DSL infrastructure.

The SHDSL.bis routers are integrated high-end Bridging/Routing capabilities with advanced functions of Multi-DMZ, virtual server mapping, VPN pass-through and QoS.

Because of rapid growth of network, virtual LAN has become one of the major new areas in internetworking industry. The SHDSL.bis routers supports the port-based and IEEE 802.1q VLAN over ATM network or EFM network.

The SHDSL.bis routers support 10Base-T /100Base-T auto-negotiation and auto-MDI/MDIX switching port to meet the enterprise need.

The SHDSL.bis routers provide advanced firewall with DoS protection, serving as a powerful firewall to protect from outside intruders of secure connection. The firewall routers also support IP precedence to classify and prioritize types of IP traffic.

The 4-port routers models support four ports 10Base-T /100Base-T auto-negotiation and auto-MDI/MDIX switching ports to meet the enterprise need.

The SHDSL.bis routers allow customers to leverage the latest in broadband technologies to meet their growing data communication needs. User can gradually migrate from ATM based access networks to Ethernet based access networks. This means the device can be installed in an existing ATM network. When the network migrates to Ethernet, the same device can be re-used in the Ethernet network without on-site intervention. The unique feature of combining ATM and EFM access in the same device leverages a smooth migration of the access network.

1.1 Features

- ✓ Support both EFM mode and ATM mode
- ✓ Easy configuration and management with password control for various application environments
- ✓ Efficient IP routing and transparent learning bridge to support Internet broadband services
- ✓ Virtual LANs (VLANs) offer significant benefit in terms of efficient use of bandwidth, flexibility, performance and
- ✓ security
- ✓ Support VPN pass-through and MPLS pass-through
- ✓ Built-in advanced SPI firewall

- ✓ Four 10/100M Base-T Auto-sensing, Auto-negotiation and Auto-MDIX switching port for flexible local area network
- ✓ connectivity (4-port Router)
- ✓ DMZ host/Multi-DMZ/Multi-NAT enables multiple workstations on the LAN to access the Internet for saving the cost of
- ✓ IP address
- ✓ Fully ATM protocol stack implementation over SHDSL
- ✓ PPPoA and PPPoE support user authentication with PAP/CHAP/MS-CHAP
- ✓ IP precedence to partition the traffic into multiple classes of service
- ✓ SNMP management with SNMPv1/SNMPv2 agent and MIB II
- ✓ Getting enhancements and new features via Internet software upgrade
- ✓ Support RSTP feature for preventing bridge loops and providing automatic backup connection
- ✓ Support Dying Gasp(Optional)
- ✓ Support TR-069(Optional)

1.2 Specification

Routing

- Support IP/TCP/UDP/ARP/ICMP/IGMP protocols
- IP routing with static routing and RIPv1/RIPv2 (RFC1058/2453)
- IP multicast and IGMP proxy (RFC1112/2236)
- Network address translation (NAT/PAT) (RFC1631)
- NAT ALGs for ICQ/NetMeeting/MSN/Yahoo Messenger
- DNS relay and caching (RFC1034/1035)
- DHCP server, client and relay (RFC2131/2132)
- IP precedence (RFC 791) (Firewall model)

Bridging

- Up to 1024 MAC address learning bridge
- IEEE 802.1D Transparent learning bridge
- IEEE 802.1q VLAN
- Port-based VLAN (4-port Router)

Security

- DMZ host/Multi-DMZ/Multi-NAT function
- Virtual server mapping (RFC1631)
- VPN pass-through for PPTP/L2TP/IPSec tunneling
- Natural NAT firewall
- Advanced Stateful Packet Inspection(SPI) firewall

- User access control: deny certain access of PCs to Internet service

Management

- Easy-to-use web-based GUI for quick setup, configuration and management
- Menu-driven interface/Command-line interface (CLI) for local console and Telnet access
- Password protected management and access control list for administration
- SNMP management with SNMPv1/SNMPv2 (RFC1157/1901/1905) agent and MIB II (RFC1213/1493)
- Software upgrade via web-browser/TFTP server

ATM/EFM

- Mode ATM/EFM
- Framing ATM, 64B/65B
- Up to 8 PVCs
- OAM F4/F5 loop back
- AAL5

ATM QoS

- UBR (Unspecified bit rate)
- CBR (Constant bit rate)
- VBR-rt (Variable bit rate real-time)
- VBR-nrt (Variable bit rate non-real-time)

AAL5 Encapsulation

- VC multiplexing and SNAP/LLC
- Ethernet over ATM (RFC 2684/1483)
- PPP over ATM (RFC 2364)
- Classical IP over ATM (RFC 1577)

PPP

- PPP over Ethernet for fixed and dynamic IP (RFC 2516)
- PPP over ATM for fixed and dynamic IP (RFC 2364)
- Support PAP/CHAP/MS-CHAP client

WAN Interface

- SHDSL.bis: ITU-T G.991.2 (2004) Annex A/B/F/G supported
- Encoding scheme: TC-PAM 16/ TC-PAM 32
- Data Rate: N x 64kbps (N=3~89, 89 as default) (2-wire Router)
- Data Rate: N x 128Kbps (N=3~89, 89 as default) (4-wire Router)
- Impedance: 135 ohm

- Compliant with IEEE 802.3ah

LAN Interface

- 4-ports switching hub (4-port model)
- 10/100 Base-T auto-sensing and auto-negotiation
- Auto-MDI/MDIX

Hardware Interface

- WAN: RJ-45 x 1
- LAN: RJ-45 x 1 (1-port Router), RJ-45 x 4 (4-port Router)
- Console: RS232 female
- Reset Button: Load factory default

Indicators

- General: PWR
- WAN: LNK, ACT
- LAN: 10M/ACT, 100M/ACT (1-port Router)
- LAN: 1, 2, 3, 4 (4-port Router)
- SHDSL.bis: ALM

Physical/Electrical

- Dimensions: 18.7 x 3.3 x 14.5cm (WxHxD)
- Power: 100~240VAC (via power adapter)
- Power consumption: 9 watts maximum.
- Temperature: 0~45°C
- Humidity: 0%~95%RH (non-condensing)

Memory

- 2MB Flash Memory, 16MB SDRAM

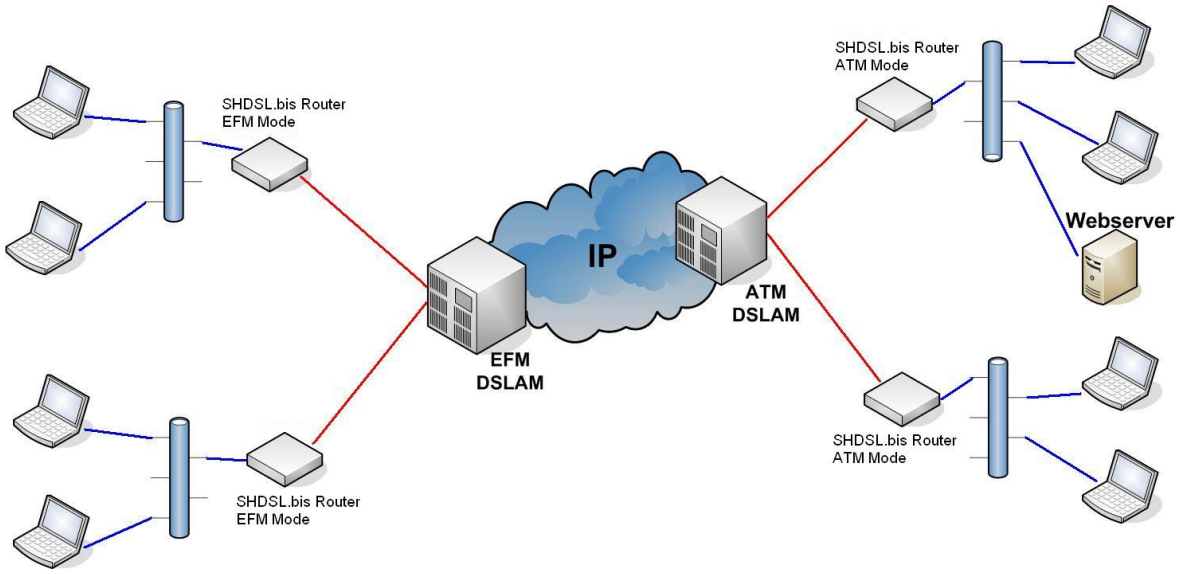
Products' Information

✧ 2-Wire G.Shdsl.bis ATM/EFM Firewall Router with 1 LAN Port

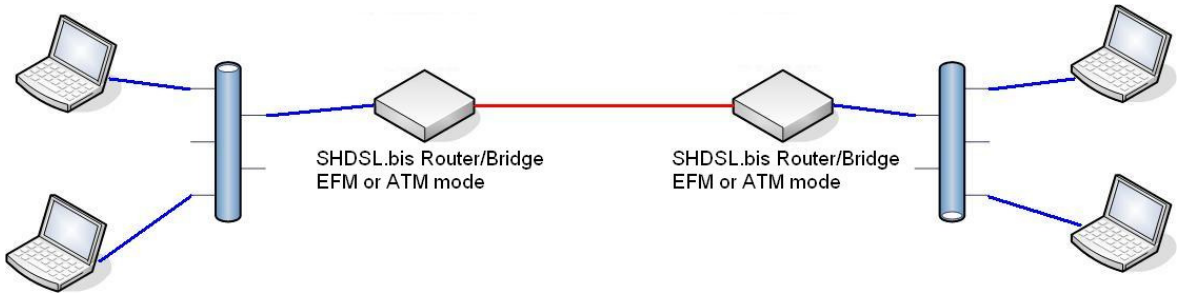
✧ 2-Wire G.Shdsl.bis ATM/EFM Firewall Router with 4 LAN Ports

✧ 4-Wire G.Shdsl.bis ATM/EFM Firewall Router with 4 LAN Ports

1.3 Applications



Combination with EFM or ATM DSLAM



Point-to-point connection

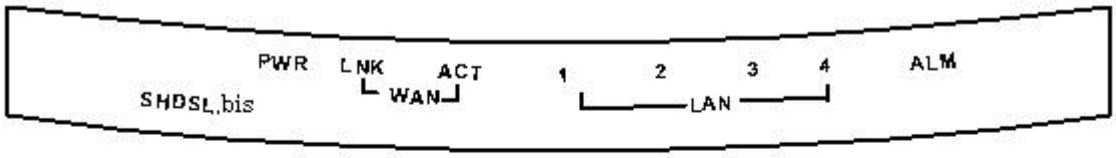
.

2 Getting to know about the router

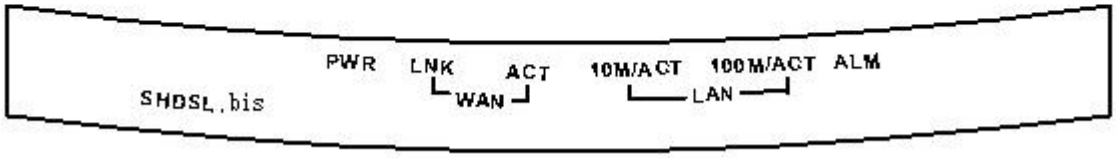
This section will introduce hardware of the router.

2.1 Front Panel

The front panel contains LEDs which show the status of the router.



Front Panel of SHDSL.bis 4-port router/bridge



Front Panel of SHDSL.bis 1-port router/bridge

LED status of SHDSL.bis 4-port router

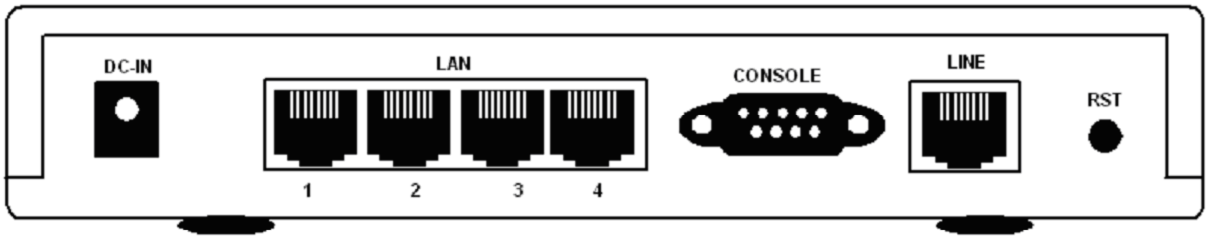
LEDs		Active	Description
PWR		On	Power on
WAN	LNK	On	SHDSL.bis line connection is established
		Blink	SHDSL.bis training
	ACT	On	Transmitting or receiving data over SHDSL.bis link
LAN	1	On	Ethernet cable is connected to LAN 1
		Blink	Transmitting or receiving data over LAN 1
	2	On	Ethernet cable is connected to LAN 2
		Blink	Transmitting or receiving data over LAN 2
	3	On	Ethernet cable is connected to LAN 3
		Blink	Transmitting or receiving data over LAN 3
	4	On	Ethernet cable is connected to LAN 4
		Blink	Transmitting or receiving data over LAN 4
ALM		On	SHDSL.bis line connection is dropped
		Blink	SHDSL.bis self test

LED status of SHDSL.bis 1-port router

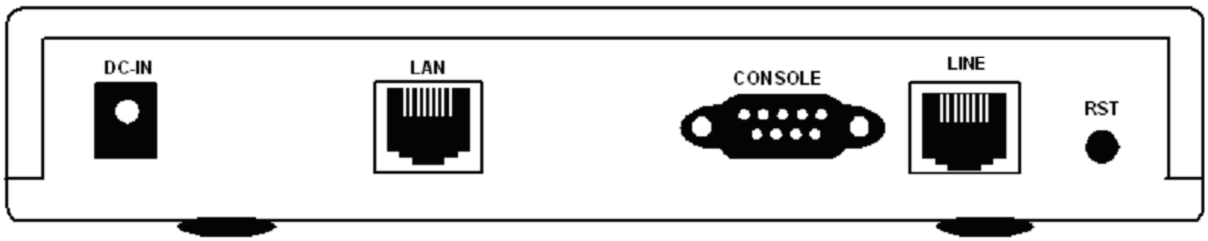
LEDs		Active	Description
	PWR	On	Power adaptor is connected to the router
WAN	LNK	On	SHDSL.bis line connection is established
		Blink	SHDSL.bis handshake
	ACT	Blink	Transmitting or receiving data over SHDSL.bis link
LAN	10M/ACT	On	LAN port connect with 10M NIC
		Blink	LAN port acts in 10M
	100M/ACT	On	LAN port connect with 100M NIC
		Blink	LAN port acts in 100M
	ALM	On	SHDSL.bis line connection is dropped
		Blink	SHDSL.bis self test

2.2 Rear Panel

The rear panel of SHDSL.bis router is where all of the connections are made.



Rear Panel of SHDSL.bis 4-wire/2-wire,4-port router/bridge



Rear Panel of SHDSL.bis 2-wire/1-port router/bridge

Connectors Description of SHDSL.bis 4-ports router

DC-IN	Power adaptor inlet: Input voltage 12VDC
LAN (1,2,3,4)	Four Ethernet10/100BaseT auto-sensing and auto-MDI/MDIX for LAN ports(RJ-45)
CONSOLE	RS- 232C (DB9) for system configuration and maintenance
LINE	SHDSL.bis interface for WAN port (RJ-45)
RST	Reset button for reboot or load factory default

Connectors Description of SHDSL.bis 1-port router

DC-IN	Power adaptor inlet: Input voltage 12VDC
LAN	Ethernet 10/100BaseT auto-sensing and auto-MDI/MDIX for LAN port (RJ-45)
CONSOLE	RS- 232C (DB9) for system configuration and maintenance
LINE	SHDSL.bis interface for WAN port (RJ-45)
RST	Reset button for reboot or load factory default

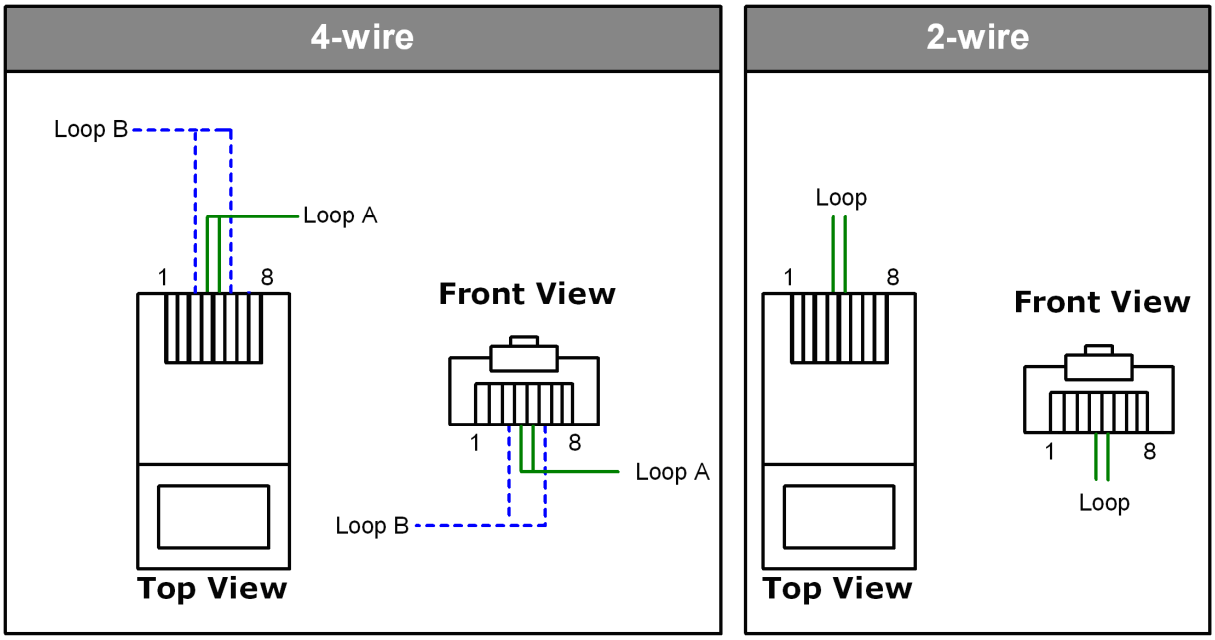
The reset button can be used only in one of two ways.

(1) Press the Reset Button for one second will cause system reboot.

(2) Pressing the Reset Button for four seconds will cause the product to load the factory default setting and lose all of your configuration. When you want to change its configuration but forget the user name or password or if the product is having problems connecting to the Internet and you want to configure it again, press the Reset Button for four seconds with a paper clip or sharp pencil.

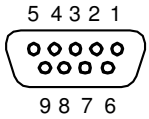
2.3 SHDSL.bis Line Connector

Below figures show the pin asignment of SHDSL.bis line cord plugs:



2.4 Console Cable

Below figure shows the pins asignment of the cosole cable:

Pin Number	Description	Figure
1	No connection	
2	RxD (O)	
3	TxD (I)	
4	No connection	
5	GND	
6	No connection	
7	No connection	
8	No connection	
9	No connection	

3 Installing the Router

This guide is designed to let users configure the G.Shdsl.bis router through Web GUI or Serial Console in the easiest and quickest way possible. Please follow the instructions carefully.

Note: There are three methods to configure the router: Serial Console, Telnet and Web Browser. Only one configuration application is used to setup the Router at any given time. Users have to choose one method to configure it.
For Web configuration, you can skip item 3.
For Serial Console Configuration, you can skip item 1 and 2.

3.1 Check List

(1) Check the Ethernet Adapter in PC or NB

Make sure that Ethernet Adapter had been installed in PC or NB for configuration of the router. TCP/IP protocol is necessary for web configuration, so please check if the TCP/IP protocol has been properly installed.

(2) Check the Web Browser in PC or NB

According to the Web Configuration, the PC or NB need to install Web Browser, IE or Firefox.
Note: Suggest to use IE8.0, Firefox V.21.0 or above and 1024x768 resolutions or above.

(3) Check the Terminal Access Program

For Serial Console and Telnet Configuration, users need to setup the terminal access program with VT100 terminal emulation.

(4) Determine Connection Setting

Users need to know the Internet Protocol supplied by the Service Provider in order to determine the mode of setting.

Protocol Selection

RFC1483	Ethernet over ATM
RFC1577	Classical Internet Protocol over ATM
RFC2364	Point-to-Point Protocol over ATM
RFC2516	Point-to-Point Protocol over Ethernet

Different Protocols requires different WAN parameters. After knowing the Protocol provided by your ISP, please also ask for the necessary WAN parameters for set up.

Bridge EoA

VPI:_
VCI:__
Encapsulation:
Gateway:
Host Name:(if applicable)

Route EoA

VPI:_
VCI:__
Encapsulation:
IP Address:
Subnet Mask:
Gateway:
DNS Server:_

IPoA

VPI:_
VCI:__
Encapsulation:
IP Address:
Subnet Mask:
Gateway:
DNS Server:_

PPPoA

VPI:_
VCI:__
Encapsulation:
User Name:
Password:
DNS Server:_
Host Name: (if applicable)

PPPoE

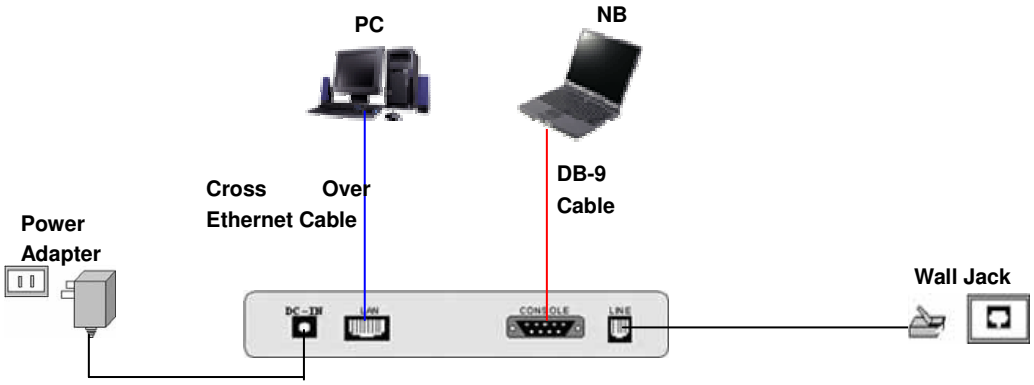
VPI:_
VCI:__
Encapsulation:
User Name:
Password:
DNS Server:_
Host Name:(if applicable)

3.2 Install the SHDSL.bis Router

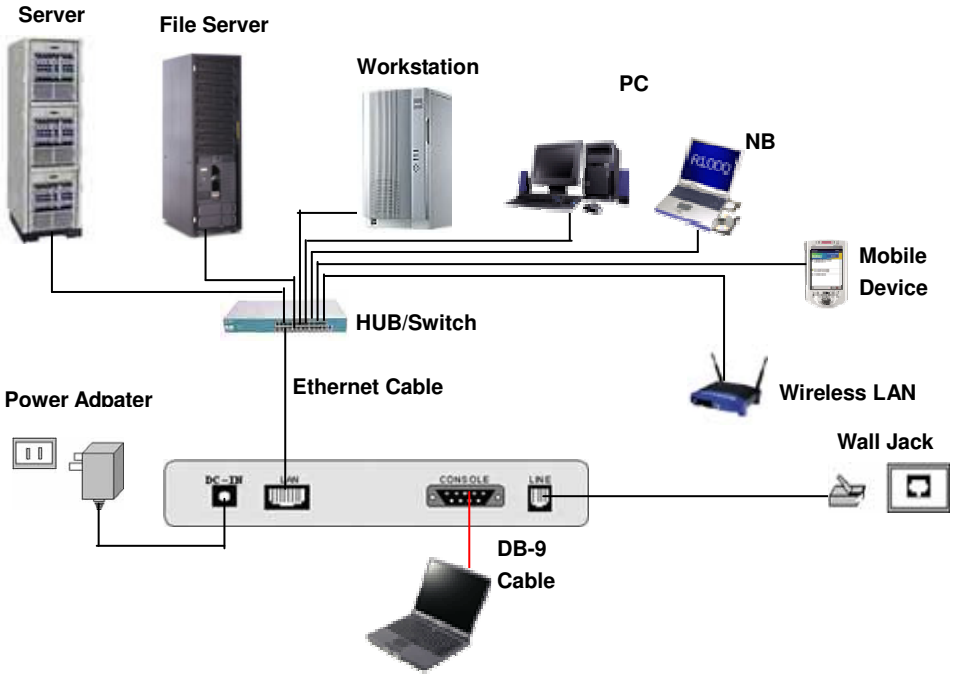
To avoid possible damage to this Router, do not turn on the router before Hardware Installation.

- Connect the power adapter to the port labeled DC-IN on the rear panel of the product.
- Connect the Ethernet cable.

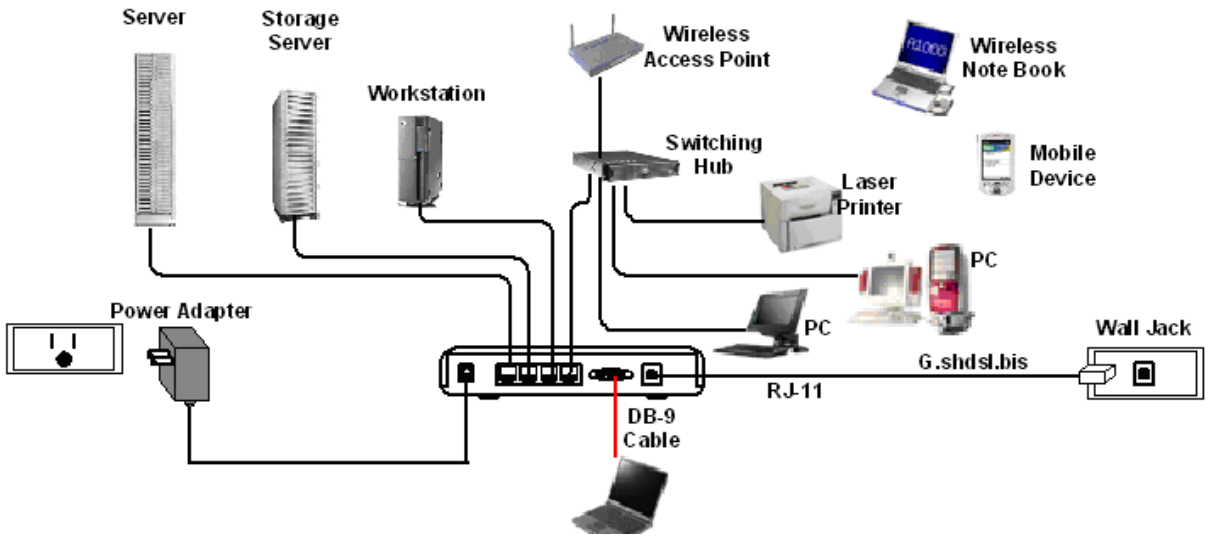
  Note: Both 1-port router and 4-port router supports auto-MDI/MDIX switching so both straight through and cross-over Ethernet cable can be used.
- Connect the phone cable to the router and the other side of phone cable to wall jack.
- Connect the power adapter to power source inlet.
- Turn on the PC or NB to configure the Router.



Direct Connection with PC or NB for SHDSL.bis 1-port router



Connection with Hub/Switch for SHDSL.bis 1-port router



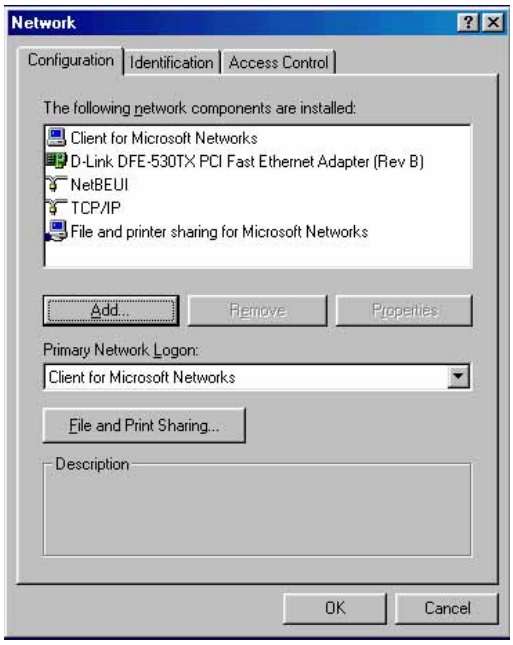
SHDSL.bis 4-port router with complex network topology

4 Configuration via Web Browser

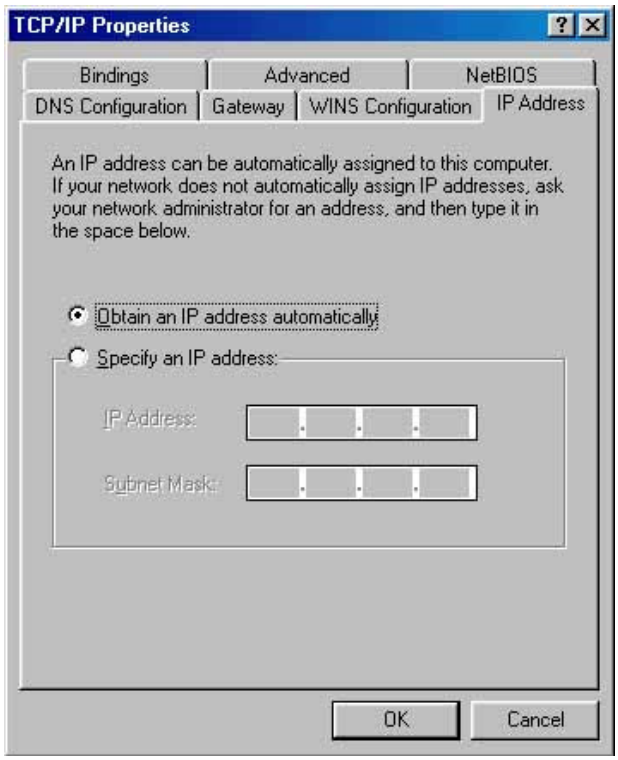
Step. 1 Click the **start** button. Select **setting** and **control panel**.

Step. 2 Double click the **network** icon.

In the Configuration window, select the **TCP/IP** protocol line that has been associated with your network card and then click **property** icon.



Choose IP address tab.
Select **Obtain IP address automatically**.
Click **OK** button.


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

The window will ask you to restart the PC. Click **Yes** button.

Cannot find server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address 192.168.0.1

After rebooting your PC, open IE or Netscape Browser to connect the Router. Type

http://192.168.0.1

The default IP address and sub net-mask of the Router is 192.168.0.1 and 255.255.255.0. Because the router acts as DHCP server in your network, the router will automatically assign IP address for PC or NB in the network.

Type User Name root and Password root and then click OK.
The default user name and password is both *root*. For the system security, suggest changing them after configuration.

Note: After changing the User Name and Password, strongly recommend you to save them because the next time when you login, the User Name and Password have to be the new ones you changed.

Function Listing

Following is the G.SHDSL.bis router full function listing.

- **BASIC (Quick Setup)**
- **ADVANCED**
  - SHDSL.bis
  - LAN
  - WAN
  - BRIDGE
  - VLAN
  - STP
  - ROUTE
  - NAT/DMZ
  - VIRTUAL SERVER
  - FIREWALL
  - IP QoS
- **STATUS**
  - SHDSL.bis
  - LAN
  - WAN
  - ROUTE
  - INTERFACE
  - FIREWALL
  - IP QoS
  - STP
- **ADMIN**
  - SECURITY
  - SNMP
  - SYSLOG
  - TIME SYNC
- **UTILITY**
  - SYSTEM INFO
  - SYSLOG
  - CONFIG TOOL
  - FIRMWARE UPGRADE
  - LOGOUT
  - RESTART

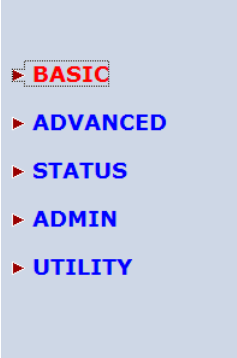
Note:

If the router is not the 4-wire model, the menu will not display the status of SHDSL.bis channel B.

4.1 Basic Setup

The Basic Setup contains Bridge or Route operation mode. Users can use it to setup the router quickly. After completing the Basic Setup, you can use the router to the access Internet or as LAN Extender. This is the easiest way to configure the router.

Note: The advanced functions are only for advanced users to configure the router. Incorrect set up of advanced functions may affect the performance, causing system error or even disconnection of the router.



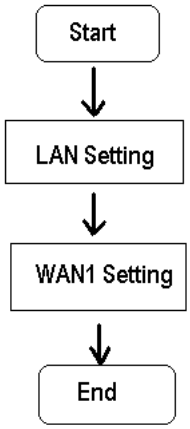
Click Basic for basic installation.

4.1.1 Bridge Mode

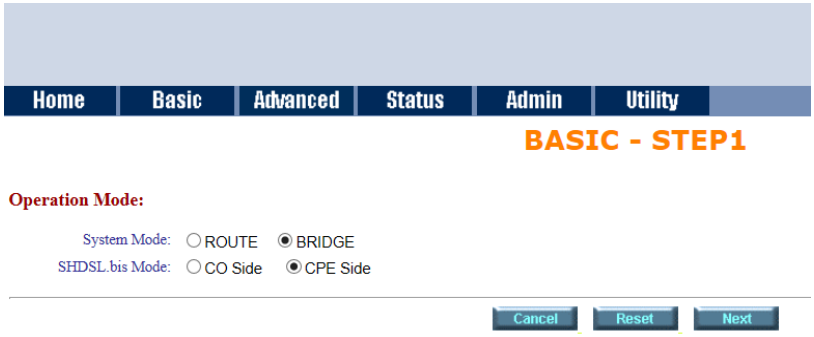
Parameter Table:

System mode	☐Route ☒Bridge	
SHDSL	☐CO side ☐CPE side	
LAN	IP address	
	Subnet Mask	
	Default Gateway	
	DNS Server 1	
	DNS Server 2	
	DNS Server 3	
	Host Name	
WAN1	VPI	
	VCI	
	Encapsulation	☐VC-mux ☐LLC

The flow chart of bridge mode setup:



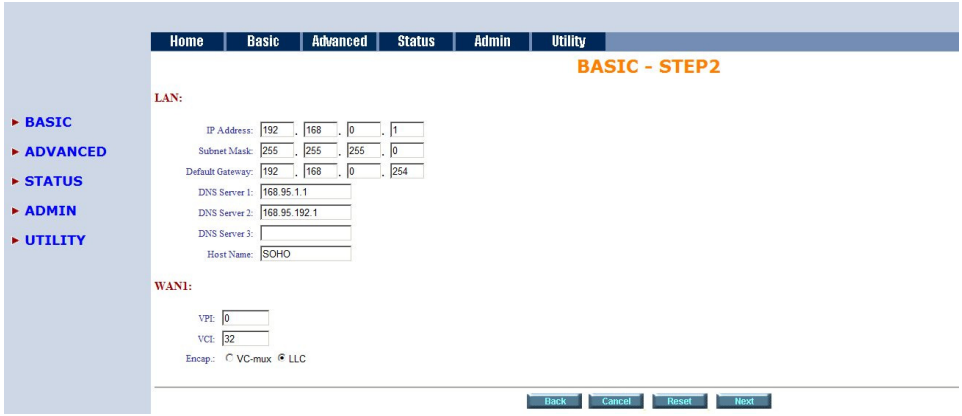
Setup up system mode and SHDSL mode



Click Bridge and CPE Side to setup Bridging mode and then click Next for the next setting.
This router can be setup as one of two SHDSL.bis working mode: CO (Central Office) and CPE (Customer Premises Equipment).

For connection with DSLAM, the SHDSL.bis router's operation mode is CPE. For "LAN to LAN" connection, one side is CO and the other side is CPE.

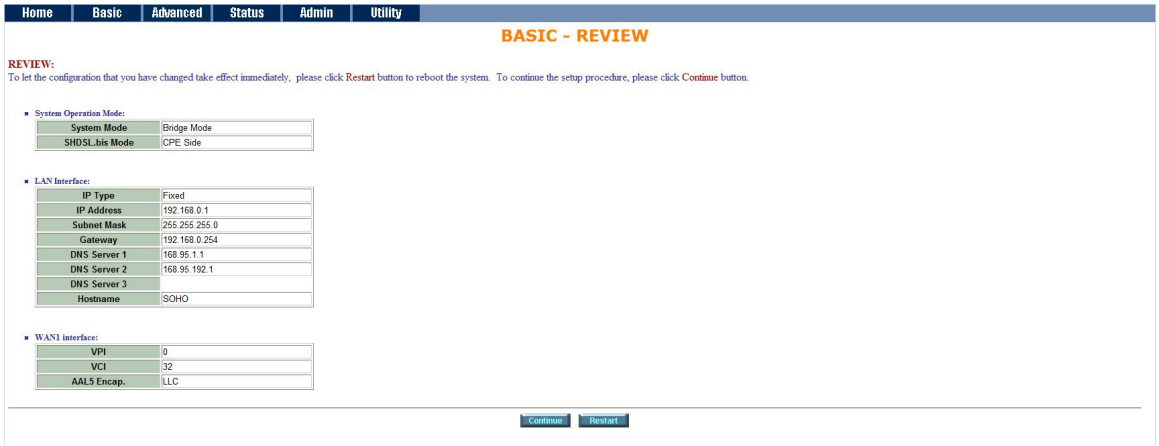
Set up (a) LAN: IP address, Subnet Mask, Default Gateway, DNS Servers and Host Name
(b) WAN1: VPI,VCI and Encapsulation



LAN:
IP: 192.168.0.1
Subnet Mask: 255.255.255.0

Gateway: 192.168.0.254 (The Gateway IP is provided by ISP.)
Host Name: SOHO
Some of the ISP requires the Host Name as identification. You may check with ISP to see if your Internet service has been configured with a host name. In most cases, this field can be ignored.
WAN1:
VPI: 0
VCI: 32
Encap: Click LLC and than Click Next to review

Review



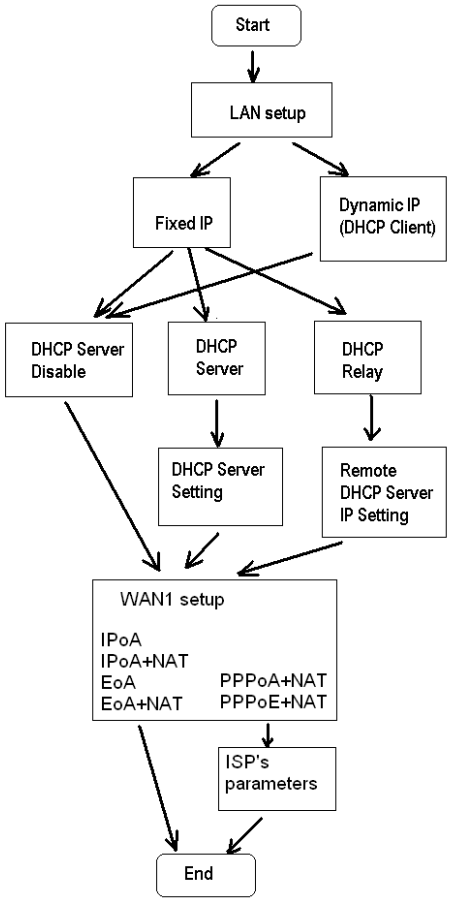
The screen will prompt the newly configured parameters. When using bridge mode, the protocol mode must be set to Ethernet over ATM (EoA). Checking the parameters and Click Restart. The router will reboot with the new setting or Continue to configure other parameters.

4.1.2 Routing Mode

Parameter Table:

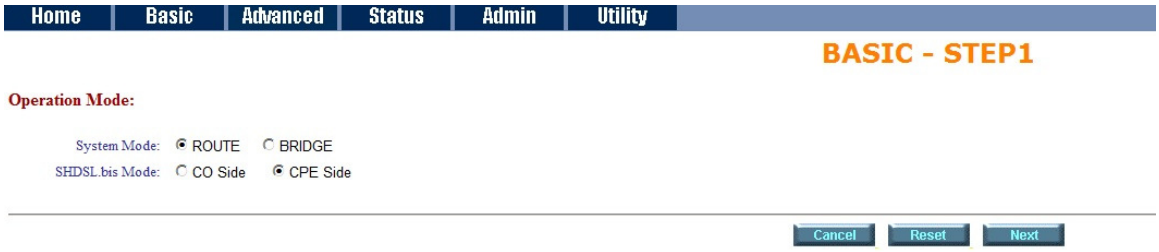
System mode	☒Route ☐Bridge			
SHDSL	☐CO side ☐CPE side			
LAN	IP type		☐Fixed ☐Dynamic(DHCP Client)	
	IP address			
	Subnet Mast			
	Host Name			
	Trigger DHCP service		☐Disable ☐Server ☐Relay	
WAN1	VPI			
	VCI			
	Encapsulation		☐VC-mux ☐LLC	
	Protocol		☐IPoA ☐IPoA + NAT ☐EoA ☐EoA + NAT ☐PPPoA + NAT ☐PPPoE + NAT	
DHCP Server	Default gateway			
	Subnet Mast			
	Start IP address			
	End IP address			
	DNS Server 1			
	DNS Server 2			
	DNS Server 3			
	Lease time			
	Host Entries	1	MAC :	IP:
		2	MAC :	IP:
		3	MAC :	IP:
		4	MAC :	IP:
		5	MAC :	IP:
		6	MAC :	IP:
		7	MAC :	IP:
		8	MAC :	IP:
		9	MAC :	IP:
		10	MAC :	IP:
DHCP Relay	IP address			

The flow chart of route mode setup:



Routing mode contains DHCP server, DHCP client, DHCP relay, Point-to-Point Protocol over ATM and Ethernet and IP over ATM and Ethernet over ATM. You have to clarify which Internet protocol is provided by ISP.

Setup up system mode and SHDSL mode



click ROUTE and CPE Side then press Next.

Set up the LAN IP address, Subnet Mask, Gateway, Host Name and Trigger DHCP Service with fixed IP type.

IP type: Fixed
IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0
Host Name: SOHO
Some of the ISPs require the host name as identification. You may check with ISP to see if your Internet service has been configured with a host name. In most cases, this field can be ignored.

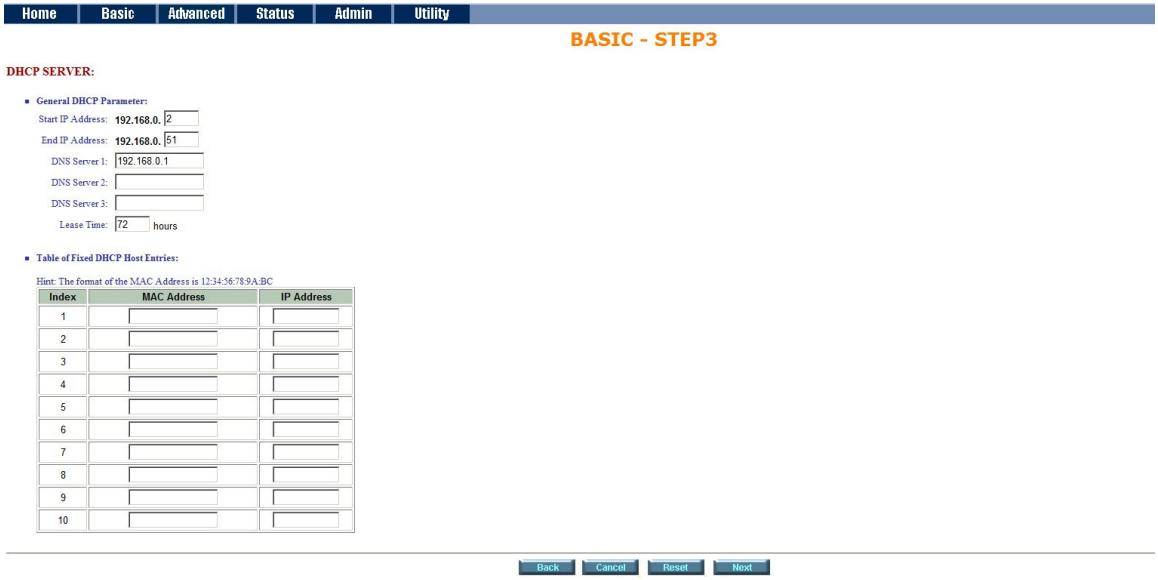
Trigger DHCP Service: Server
The default setup is Enable DHCP server. If you want to turn off the DHCP service, choose Disable.

If set DHCP server to Relay, the router acts as a surrogate DHCP server and relays requests and responses between the remote server and the clients.

DHCP Server
Dynamic Host Configuration Protocol (DHCP) is a communication protocol that lets network administrators to manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet Protocol, each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine.
Without DHCP, the IP address must be entered manually at each computer. If computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator to supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

If the DHCP server is “Enable”, you have to setup the following parameters for processing it as DHCP server.
The embedded DHCP server assigns network configuration information at most 253 users accessing the Internet at the same time.

Setup the DHCP Server parameters and fixed DHCP host table



Start IP Address: This field specifies the first of the contiguous addresses in the IP address pool.
End IP Address: The field specifies the last of the contiguous addresses in the IP address pool.

For example: If the LAN IP address is 192.168.0.1, the IP range of LAN is 192.168.0.2 to 192.168.0.51. The DHCP server assigns the IP form Start IP Address to End IP Address. The legal IP address range is form 0 to 255, but 0 are reserved as network name and 255 are reserved for broadcast. It implies the legal IP address range is from 1 to 254. That means you cannot assign an IP greater than 254 or less then 1. **Lease time** 72 hours indicates that the DHCP server will reassign IP information in every 72 hours.

DNS Server1, **DNS Server2** and **DNS Server3**: Your ISP will provide at least one Domain Name Service Server IP. You can type the router IP in this field. The router will act as DNS server relay function. There are three DNS servers to be used.
You may assign a fixed IP address to some device while using DHCP, you have to put this device's MAC address in the **Table of Fixed DHCP Host Entries**. There are ten fixed IP address locations that can be used.
Every Ethernet device has a unique MAC(Media Access Control) address. The MAC address is assigned at factory and consists of six pairs of hexadecimal characters, for example, 00:03:79:0A:01:3F

Press Next to setup WAN1 parameters.

Some of the ISP provides DHCP server service by which the PC in LAN can access IP information automatically. To setup the DHCP client mode, please follow the procedure.

Set up IP address, Subnet Mask, Host Name with DHCP Client mode

LAN IP Type: Dynamic(DHCP Client)

Click Next to set up WAN1 parameters.

DHCP relay

If you have a DHCP server in LAN and you want to use it for DHCP services, the product provides DHCP relay function to meet your need.

IP Type: Fixed

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

Host Name: SOHO

Some of the ISPs require the host name as identification. You may check with your ISP to see if your Internet service has been configured with a host name. In most cases, this field can be ignored.

Trigger DHCP Service: Relay

Set up the DHCP Server

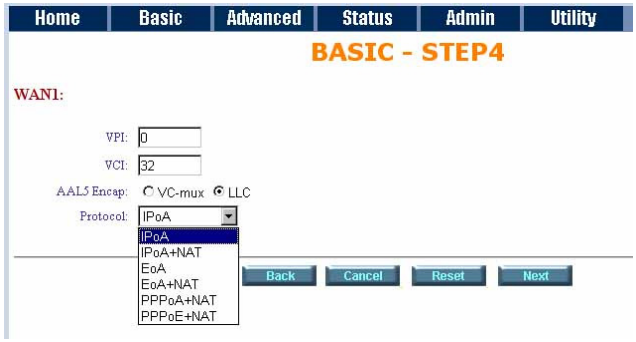
Press Next to setup **Remote DHCP server parameter**.

When using DHCP relay service, the remote DHCP server IP address must be entered.

Enter DHCP server IP address in IP address field.

Press Next

Set up the WAN1 VPI, VCI Encap. and Protocol



VPI: 0
VCI: 33
AAL5 Encap: LLC
Protocol: PPPoA + NAT or PPPoE + NAT
Click Next to setup User name and password.
For more understanding about NAT, review NAT/DMZ chapter.

If the Protocol using PPPoA+NAT or PPPoE+NAT, you must setup the ISP's parameters on the following:

Type the ISP1 parameters.
Username: test
Password: test
Password Confirm: test
Your ISP will provide the user name and password.
Idle Time: 10

You want your Internet connection to remain on at all time, enter "0" in the Idle Time field.
IP Type: Dynamics.
The default IP type is Dynamic. It means that ISP PPP server will provide IP information including dynamic IP address when SHDSL.bis connection is established. On the other hand, you do not need to type the IP address of WAN1. Some of the ISP will provide fixed IP address over PPP. For fixed IP address:
IP Type: Fixed
IP Address: 192.168.1.1
Click Next.
Note: For safety, the password will be prompt as star symbol.

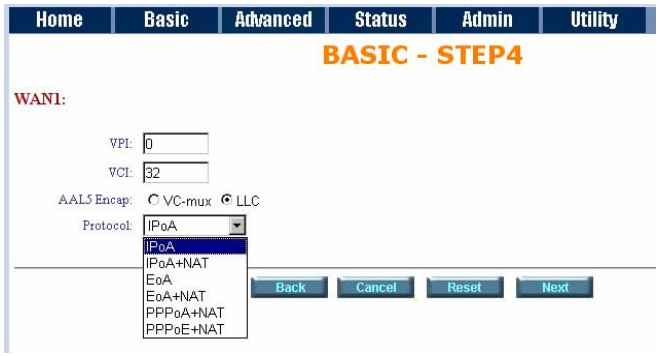
***Username** : Enter the user name exactly as your ISP assigned.*
***Password**: Enter the password associated with the user name above.*

***Password confirm**: Enter the password again for confirmation.*
***Idle Time**: When you don't want the connection up all the time and specify an idle time on this field.*
***IP type**: A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a differnet one each time you connect to the Internet.*

The screen will prompt the parameters that will be written in NVRAM. Check the parameters before writing in NVRAM.

Press Restart to restart the router working with new parameters or press to continue fir setting another parameter.

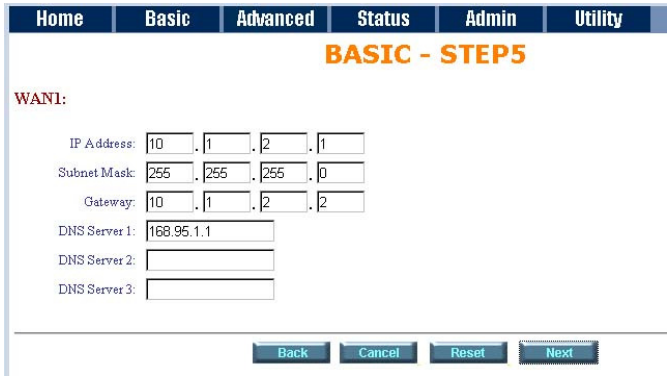
Set up : WAN1 VPI, VCI, Encap. and Protocol



WAN:
VPI: 0
VCI: 33
AAL5 Encap: LLC
Protocol: IPoA , EoA , IPoA + NAT or EoA + NAT
Click Next to setup the IP parameters.

For more understanding about NAT, review NAT/DMZ chapter.

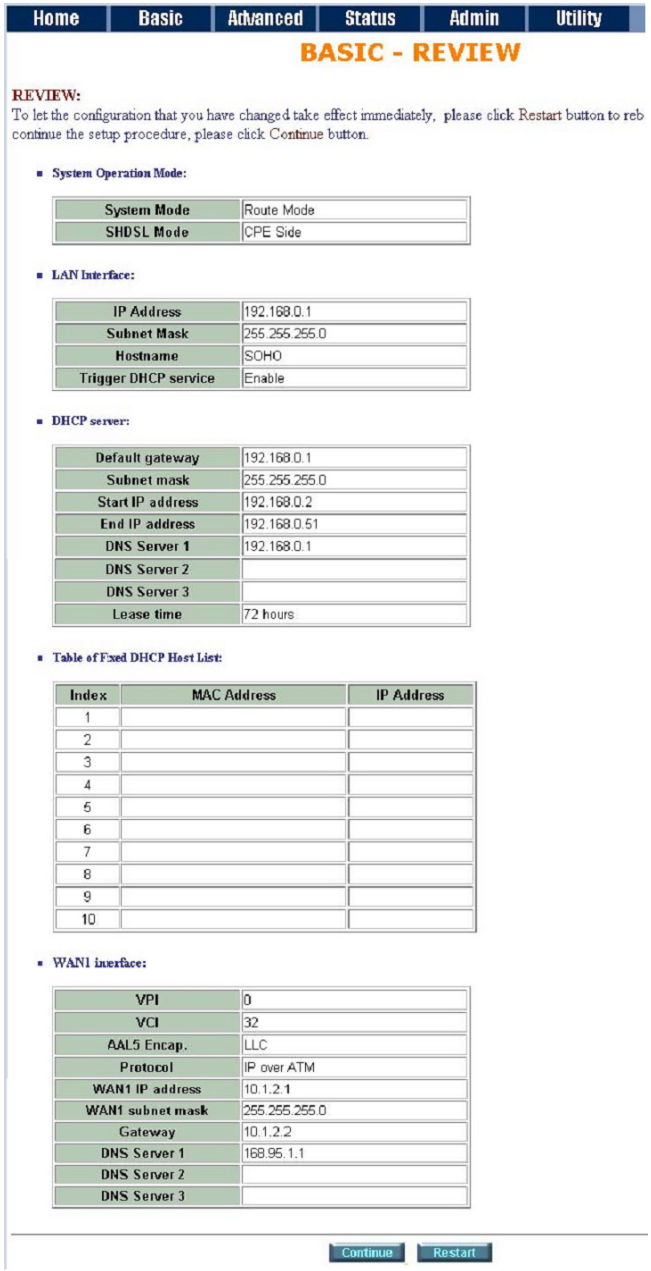
Set up the WAN1 IP address, Subnet Mask, gateway and DNS Server



IP Address: 10.1.2.1
It is router IP address like from Internet. Your ISP will provide it and you need to specify here.
Subnet mask: 255.255.255.0
This is the router subnet mask seen by external users on Internet. Your ISP will provide it to you.
Gateway: 10.1.2.2
Your ISP will provide you the default gateway.
DNS Server 1: 168.95.1.1
Your ISP will provide at least one DNS (Domain Name System) Server IP address.

Click Next to review.

Review



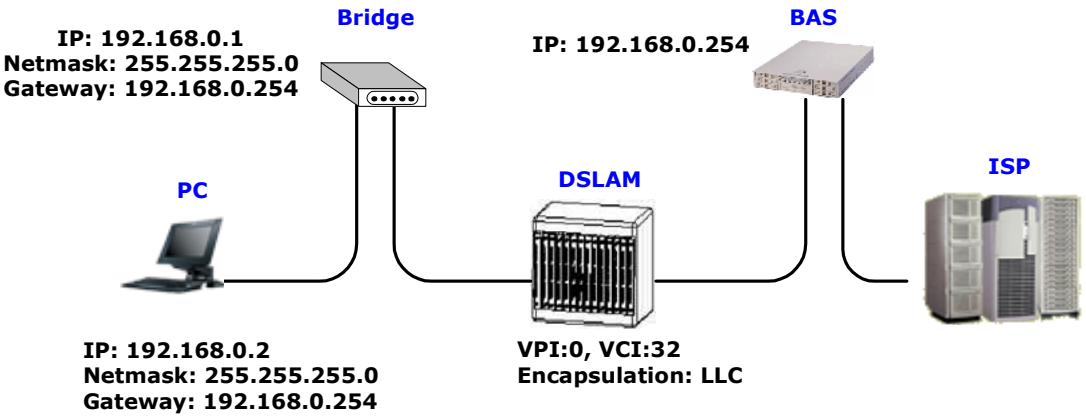
The screen will prompt the parameters that will be written in NVRAM. Check the parameters before writing in NVRAM.

Press Restart to restart the router working with new parameters or press **Continue** to setup another parameter.

4.1.3 Reference diagram

Bridge mode

When configured in Bridge Mode, the router will act as a pass-through device and allow the workstations on your LAN to have public addresses directly on the internet.

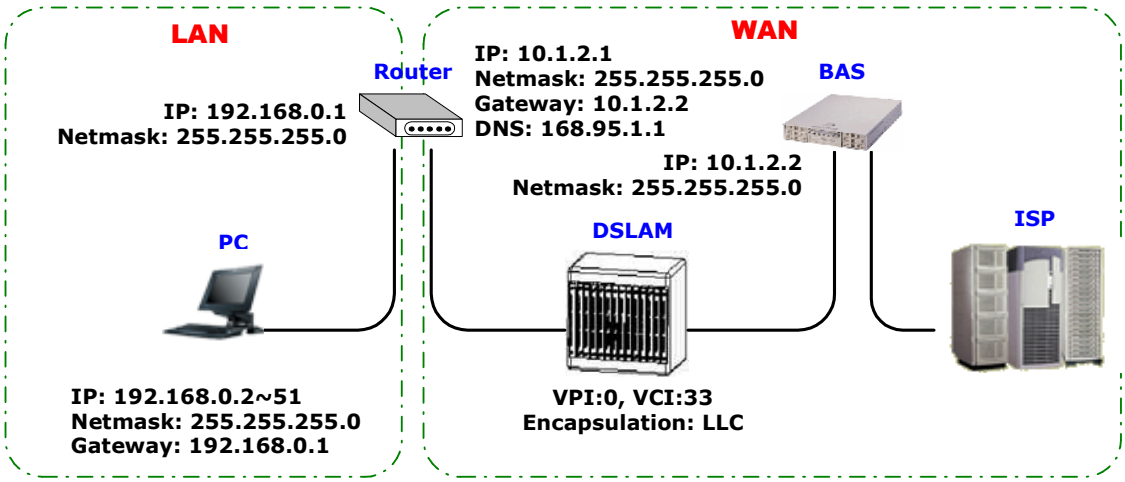


IPoA or EoA

IPoA (Dynamic IP over ATM) interfaces carries IP packets over AAL5. AAL5 provides the IP hosts on the same network with the data link layer for communications. In addition, to allow these hosts to communicate on the same ATM networks, IP packets must be tuned somewhat. AS the bearer network of IP services, ATM provides high speed point-to-point connections which considerably improve the bandwidth performance of IP network. On the other hand, ATM provides excellent network performance and perfect QoS.

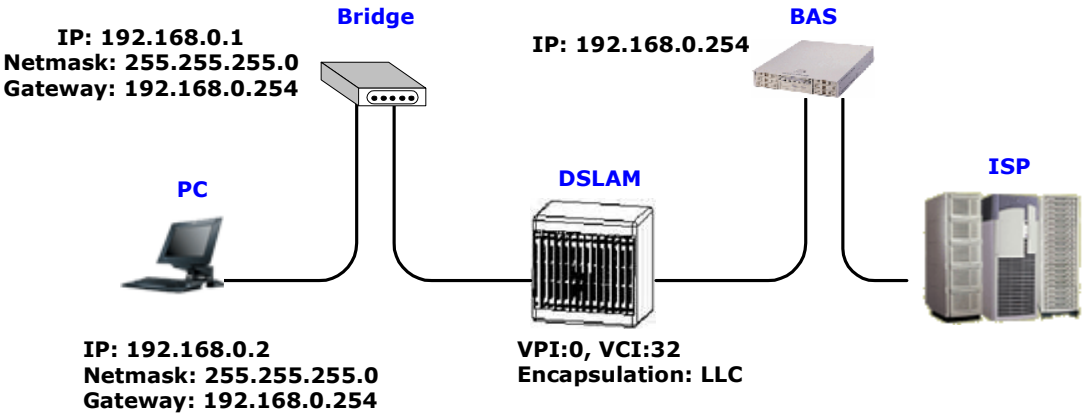
EoA (Ethernet-over-ATM) protocol is commonly used to carry data between local area networks that use the Ethernet protocol and wide-area networks that use the ATM protocol. Many telecommunications industry networks use the ATM protocol. ISPs who provide DSL services often use the EoA protocol for data transfer with their customers' DSL modems.

EoA can be implemented to provide a bridged connection between a DSL modem and the ISP. In a bridged connection, data is shared between the ISP's network and their customer's as if the networks were on the same physical LAN. Bridged connections do not use the IP protocol. EoA can also be configured to provide a routed connection with the ISP, which uses the IP protocol to exchange data.



PPPoE or PPPoA

PPPoA (point-to-point protocol over ATM) and PPPoE (point-to-point protocol over Ethernet) are authentication and connection protocols used by many service providers for broadband Internet access. These are specifications for connecting multiple computer users on an Ethernet local area network to a remote site through common customer premises equipment, which is the telephone company's term for a modem and similar devices. PPPoE and PPPoA can be used to office or building. Users share a common Digital Subscriber Line (DSL), cable modem, or wireless connection to the Internet. PPPoE and PPPoA combine the Point-to-Point Protocol (PPP), commonly used in dialup connections, with the Ethernet protocol or ATM protocol, which supports multiple users in a local area network. The PPP protocol information is encapsulated within an Ethernet frame or ATM frame.



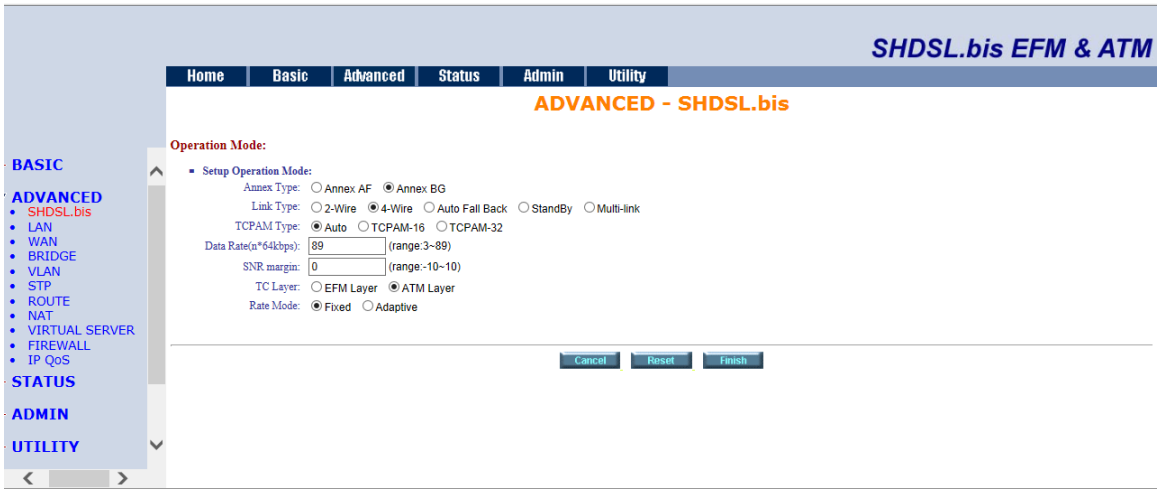
4.2 Advanced Setup

Advanced setup contains **SHDSL.bis, LAN, WAN, Bridge, VLAN, Ethernet, Route, NAT/DMZ, Virtual SERVER, FIREWALL and IP QoS** parameters.

4.2.1 SHDSL.bis

You can setup the Annex type, data rate and SNR margin for SHDSL.bis parameters in SHDSL.bis. Click SHDSL.bis

Enter Parameters in SHDSL.bis



4.2.1.1 Annex Type

There are two Annex types: **Annex AF** and **Annex BG** . If the router will connect to your ISP, please check with them for the correct setting. If your routers are configured for point to point application, you must choose one of the two types according to which line rate you need.

4.2.1.2 Line Type

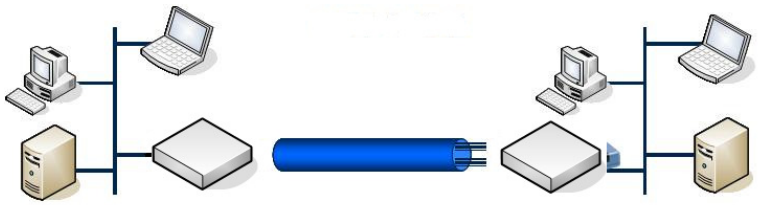
There are five Line Types for you to choose: **2-Wire**, **4-Wire**, **Auto Fall Back**, **StandBy** and **Multi-link.**

2-Wire mode

2-wire router will provide data rate up to 5.696Mbps. For 4-wires model, it will only use the first pair for single-pair DSL wire application.

4-Wire mode

4-wire router will provide data rate up to 11.392Mbps.



In this mode, each wire pairs of SHDSL.bis router must be configured with the same line rate. If one pair fails then the entire line must be restarted.

Auto Fall Back Mode

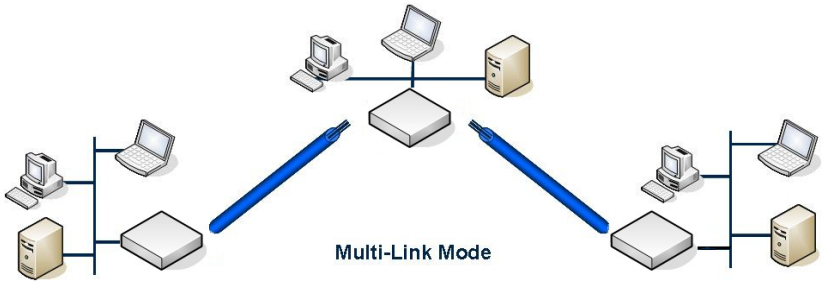
Two DSL pairs are working simultaneously. When one pair is disconnected, the other pair will keep working.

Stanby Mode

Only one of two pairs are working, the other pair is standby as back up. If the working pair fails, the standby pair will start up.

Multi–Link Mode

For 4-Wire model, each pair will connect to a different remote device, which may or may not be in the same location. The routers can be used to create a daisy chain or ring network.



4.2.1.3 TCPAM Type

TCPAM stands for Trellis Coded Pulse Amplitude Modulation. It is the modulation format that is used in both HDSL2 and SHDSL, and provides robust performance over a variety of loop conditions. SHDSL.bis supports 16 level TCPAM line code(TPCAM-16) or 32 level TCPAM line code(TCPAM-32) to provide a rate/reach adaptive capability, offering enhanced performance (increased rate or reach) and improved spectral compatibility. The default option is Auto. You may assign the different type manually by clicking the caption TPCAM-16 or TPCAM-32. Only Annex AF and BG can apply TCPAM-32.

4.2.1.4 Data Rate

For 2-wire model **(n*64kbps)**

You can setup the SHDSL.bis data rate in the multiple of 64kbps.
The default data rate is 5696Kbps (n=89).
For using Annex AF or BG
TCPAM32 ; data rate is 192Kbps ~ 5696Kbps (Nx64kbps, N=3~89)
TCPAM16 ; data rate is 192Kbps ~ 3840Kbps (Nx64kbps, N=3~60)

For 4-wire model **(n*128kbps)**

You can setup the SHDSL.bis data rate in the multiple of 128kbps.
The default data rate is 11392Kbps (n=89).
For using Annex AF or BG
TCPAM32 ; data rate is 384Kbps ~ 11392Kbps (Nx128kbps, N=3~ 89)
TCPAM16 ; data rate is 384Kbps ~ 7680Kbps (Nx128kbps, N=3~60)

		2-wire model	4-wire model
Annex AF/BG	TCPAM-16	192~3840 kpbs	384~7680 kbps
	TCPAM-32	192~5696 kpbs	384~11392 kbps

4.2.1.5 SNR Margin

This is an index for line connection quality. You can see the actual SNR margin in STATUS SHDSL.bis. The larger the SNR margin, the better the line connection quality.
The range of SNR Margin is -10 to 21.

If you set SNR margin in the field as 3, the SHDSL.bis connection will drop and reconnect when the SNR margin is lower than 3. The device will reduce the line rate and reconnect for better line connection quality.

4.2.1.6 TC Layer

There are two TC layer setting on this router: EFM layer and ATM layer. It is based on the networks connected: ATM-based Access Network or Ethernet-based Access Network.

4.2.1.7 Rate Mode

For adaptive mode, you have to configure it in rate mode. The router will adapt the optimal data rate according to the line status.

The screen will prompt the parameters that will be written in NVRAM. Check the parameters before writing in NVRAM.
Press Restart to restart the router working with new parameters or press continue to setup another parameter.

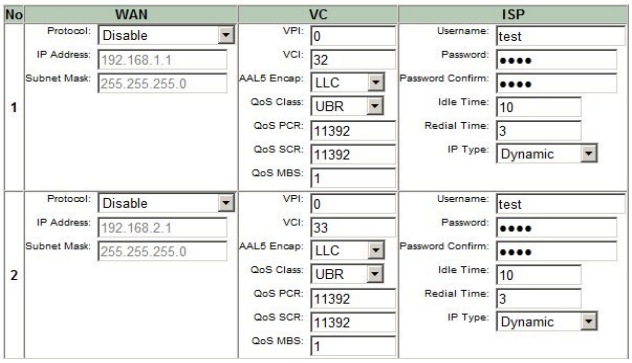
4.2.2 WAN

The router can support up to 8 PVCs. WAN 1 was configured via **BASIC** menu except QoS. If you want to setup another PVCs such as WAN 2 to 7, those parameters can be configured on the pages of WAN under ADVANCED. On the other hand, you don't need to setup WAN unless you apply two or more Internet Services with ISPs.

The parameters in WAN Number 1 has been setup in Basic Setup.
If you want to setup additional PVCs, you can configure WAN 2 to WAN 8.

WAN Interface Parameters:

- **Table of Current WAN Interface Parameter:**



Enter the parameters:

Protocol: If WAN Protocol is PPPoA or PPPoE with dynamic IP, leave the default WAN IP Address and Subnet Mask as default setting. The system will ingore the IP Address and Subnet Mask information, but leaving blanks in default setting will cause system error.

If the WAN Protocol is IPoA or EoA, leave the ISP parameters as default setting. The system will ingore the information, but leaving blanks in default setting will cause system error.

VC-mux (VC-based Multiplexing): Each protocol is assigned to a specific virtual circuit. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

LLC (LLC-based Multiplexing): One VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantagrous if it is not practical to have a sepatate VC for each carried protocol.

VPI (Virtual Path Identifier) is for set up ATM Permanent Virtual Channels (PVC).The valid range for VPI is 0 to 255.

VCI (Virtual Channel Identifier is for set up ATM Permanent Virtual Channels (PVC). The valid range for VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic.)

QoS (Quality of Service) **class** : The Traffic Management Specification V4.0 defines ATM service cataloges that describe both the traffic transmitted by users onto a network as well as the Quailty of Service that the network needs to provide for that traffic. There are four classes to be selected: UBR, CBR, rt-VBR and nrt-VBR. Select CBR to specify fixed bandwidth for voice or data traffic. Select UBR for applications that are not time-sensitive such as e-mail. Select VBR for bursty traffic and bandwidth sharing with other applications.

UBR (Unspecified Bit Rate) is the simplest service provided by ATM networks. There is no guarantee of anything. It is a primary service used for transferring Internet traffic over the ATM network.

CBR (Constant Bit Rate) is used by connections that require a static amount of bandwidth that is available during the connection life time. This bandwidth is characterized by Peak Cell Rate (PCR). Based on the PCR of the CBR traffic, specific cell slots are assigned for the VC in the schedule table. The ATM always sends a single cell during the CBR connection's assigned cell slot.

VBR-rt (Varible Bit Rate real-time) is intended for real-time applications, such as compressed voice over IP and video comferencing, that require tightly constrained delays and delay variation. VBR-rt is characterized by a peak cell rate (PCR), substained cell rate (SCR), and maximun burst rate (MBR).

VBR-nrt (Varible Bit Rate non-real-time) i*s intended for non-real-time applications, such as FTP, e-mail and browsing.*

PCR (Peak Cell Rate) in kbps: The maximum rate at which you expect to transmit data, voice and video. Consider PCR and MBS as a menas of reducing lantency, not increasing bandwidth. The range of PCR is 384kbps to 11392kbps

SCR (Substained Cell Rate): The sustained rate at which you expect to transmit data, voice and video. Consider SCR to be the true bandwidth of a VC and not the long-term average traffic rate. The range of SCR is 384kbps to 11392kbps.

MBS (Maximum Burst Size): Refers to the maximum number of cells that can be sent at the peak rate. The range of MBS is 1 cell to 255 cells.

Username : Enter the user name exactly as your ISP assigned.

Password: Enter the password associated with the user name above.

Password confirm: Enter the password again for confirmation.

Idle Time: You can specify an idle time on this field when you don't want the connection up all the time.

IP type: A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a differnet one each time you connect to the Internet.

Press Finish to finish setting.

The screen will prompt the parameters that will be written in NVRAM. Check the parameters before writing in NVRAM.

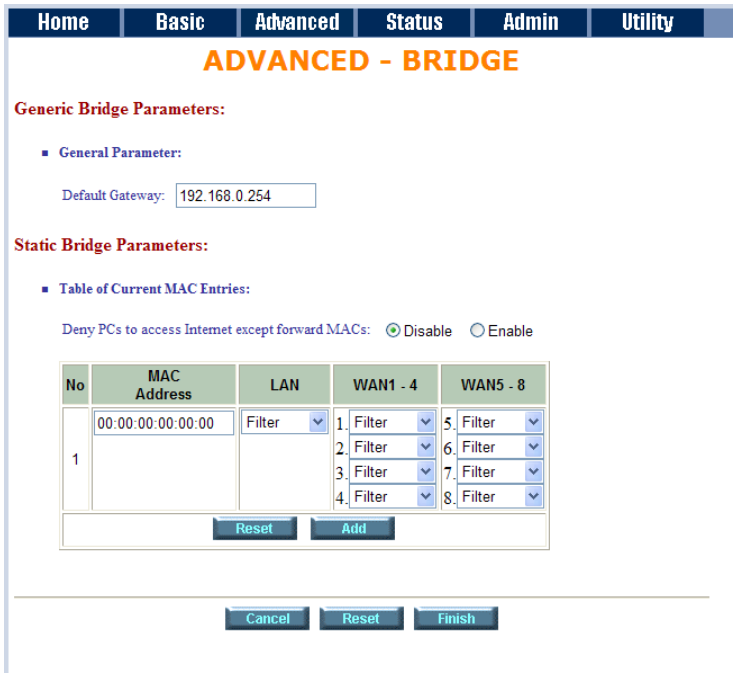
Press Restart to restart the router working with new parameters or press continue to setup other parameters.

4.2.3 Bridge

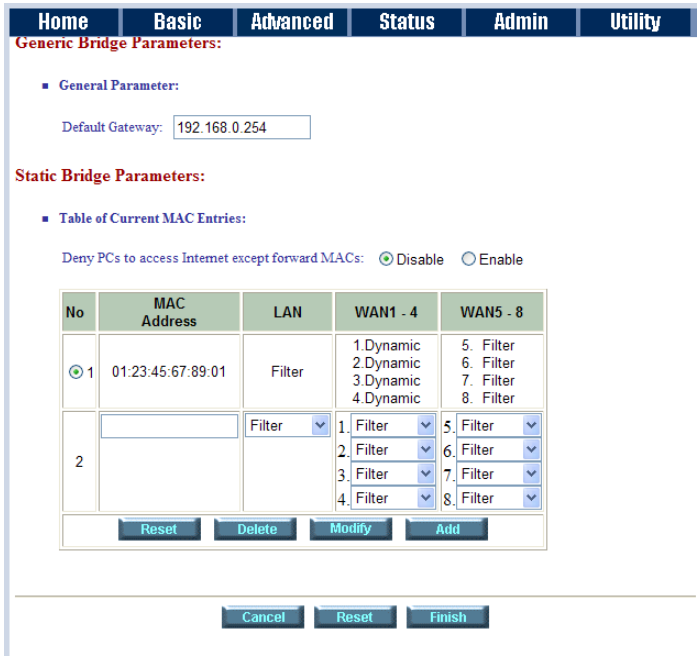
If you want to setup advanced filter function while router is working in bridge mode, you can use **BRIDGE** menu to setup the filter/blocking function.

Click Bridge to setup.

BASIC
ADVANCED
SHDSL.bis
LAN
WAN
BRIDGE
VLAN
STP
ROUTE
NAT
VIRTUAL SERVER
FIREWALL
IP QoS
STATUS
ADMIN
UTILITY


Home
Basic
Advanced
Status
Admin
Utility
ADVANCED - BRIDGE
Generic Bridge Parameters:
General Parameter:
Default Gateway: 192.168.0.254
Static Bridge Parameters:
Table of Current MAC Entries:
Deny PCs to access Internet except forward MACs: Disable Enable
No
MAC Address
LAN
WAN1 - 4
WAN5 - 8
1
00:00:00:00:00:00
Filter
1. Filter
2. Filter
3. Filter
4. Filter
5. Filter
6. Filter
7. Filter
8. Filter
Reset
Add
Cancel
Reset
Finish

Press Add on the bottom of web page to add the static bridge information.

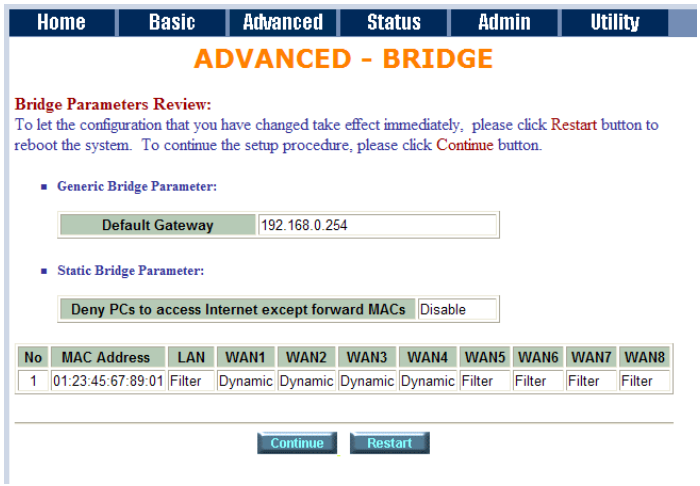


If you want to filter the designated MAC address of LAN PC to access Internet, press Add to establish the filtering table. Put the MAC address in **MAC Address** field and select Filter in **LAN** field.

If you want to filter the designated MAC address of WAN PC to access LAN, press Add to establish the filtering table. Key the MAC address in **MAC Address** field and select Filter in WAN field.

For example: if your VC is setup at WAN 1, select WAN 1 Filter.

Press Finish on the bottom of web page to review the bridge parameters.



The screen will prompt the parameters that will be written in NVRAM. Check the parameters before writing in NVRAM.

Press Restart to restart the router working with new parameters or press Continue to setup another parameter.

4.2.4 VLAN

Click VLAN to configure VLAN.

VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group.

With MTU (Multi-Tenant Unit) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN.

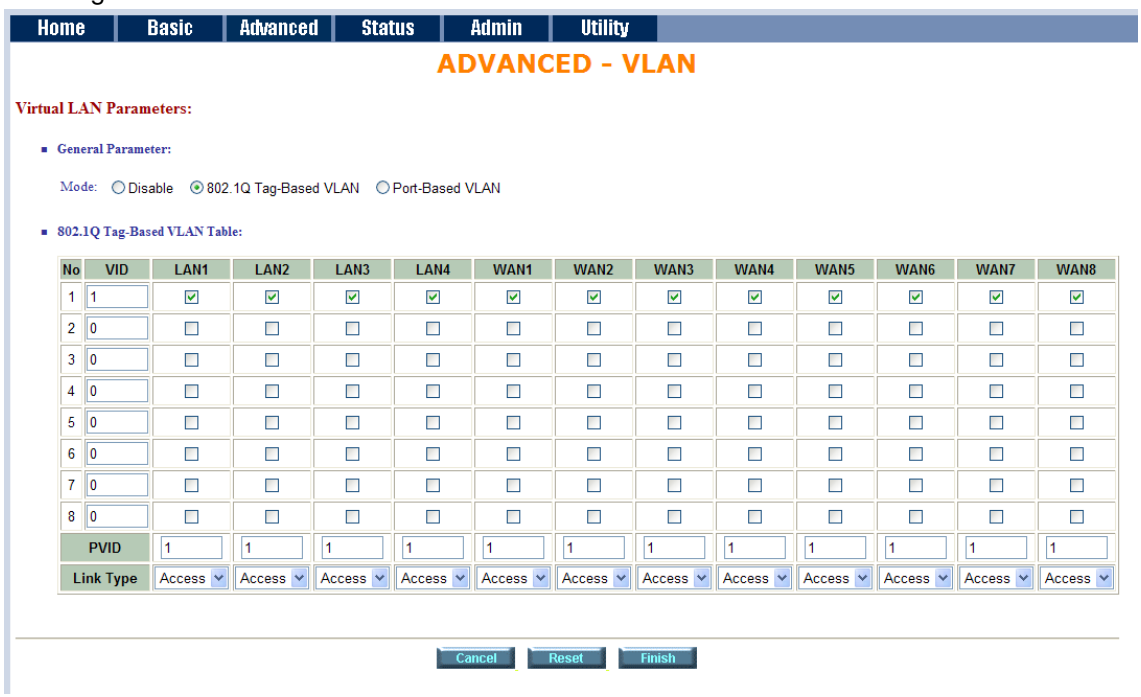
VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

The IEEE 802.1Q defines the operation of VLAN bridges that permit the definition, operation, and administration of VLAN topologies within a bridged LAN infrastructure.

The router supports two types of VLAN: **802.1Q Tag-Based VLAN** and **Port-Based VLAN**.
User can configure one of them to the router.

4.2.4.1 802.1Q Tag-Based VLAN

For setting 802.1Q VLAN click the 802.1Q Tagt-Based VLAN. The screem will prompt as the following.



VID: (Virtual LAN ID) It is a definite number of ID range from 1 to 4094.
PVID: (Port VID) It is an untagged member from 1 to 4094 of default VLAN.
Link Type: Access means the port can receive or send untagged packets.
Trunk means that the prot can receive or send tagged packets.

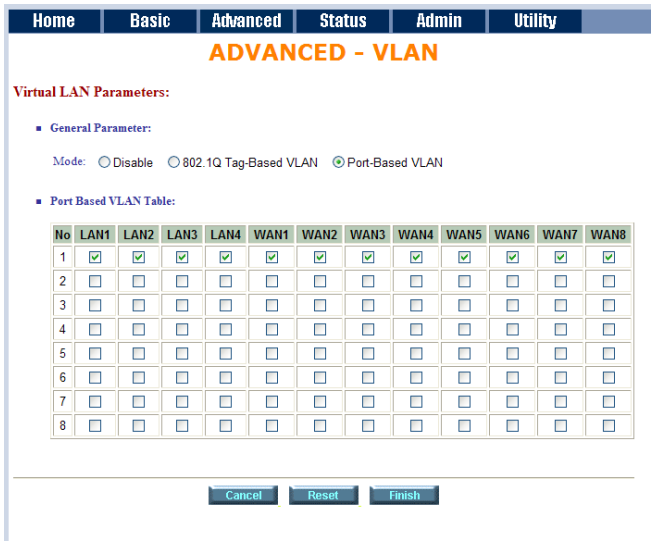
By default, the router initially configures one VLAN, VID=1.
A port such as LAN1 to LAN4 and WAN1 to WAN8 can have only one PVID, but can have as many VIDs as the router can store in the VLAN table.

Ports in the same VLAN group share the same frame broadcast domin thus increase network performance through reduced boardcast traffic. VLAN groups can be modified at any time by adding, moving or changing ports without any re-cabling.

4.2.4.2 Port-Based VLAN

Port-Based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

For setting Port-Based VLAN, Click Port-Based VLAN, The screem will prompt as follows:



Port-Based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

When using the port-based VLAN, the port is assigned to a specific VLAN independent of the user or system attached to the port. This means all users attached to the port should be members in the same VLAN. The network administrator typically performs the VLAN assignment. The port configuration is static and cannot be automatically changed to another VLAN without manual reconfiguration.

As with other VLAN approaches, the packets forwarded using this method do not leak into other VLAN domains on the network. After a port has been assigned to a VLAN, the port cannot send to or receive from devices in another VLAN.

▪ Port Based VLAN Table:

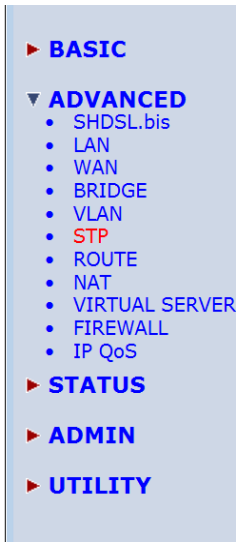
No	LAN1	LAN2	LAN3	LAN4	WAN1	WAN2	WAN3	WAN4	WAN5	WAN6	WAN7	WAN8
1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

The default setting is all ports (LAN1 to LAN4 and WAN1 to WAN8) connected together which means all ports can communicate with each other. That is, there are no virtual LANs. The option is the most flexible but the least secure.

▪ Port Based VLAN Table:

No	LAN1	LAN2	LAN3	LAN4	WAN1	WAN2	WAN3	WAN4	WAN5	WAN6	WAN7	WAN8
1	☑	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐
2	☐	☑	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐
3	☐	☐	☑	☐	☐	☐	☑	☐	☐	☐	☐	☐
4	☐	☐	☐	☑	☐	☐	☐	☑	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

4.2.5 STP



This Web page allows you to configure Bridge STP Parameters as Disable, STP or RSTP.

STP (Spanning-Tree Protocol) defined in the IEEE 802.1D, is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For an Ethernet network to function properly, only one active path can exist between two stations.

Multiple active paths between stations cause loops in the network. If a loop exists in the network topology, the potential exists for duplication of messages. When loops occur, some switches see stations appear on both sides of the switch. This condition confuses the forwarding algorithm and allows duplicate frames to be forwarded.

To provide path redundancy, Spanning-Tree Protocol defines a tree that spans all switches in an extended network. Spanning-Tree Protocol forces certain redundant data paths into a standby (blocked) state. If one network segment in the Spanning-Tree Protocol becomes unreachable, or if Spanning-Tree Protocol costs change, the spanning-tree algorithm reconfigures the spanning-tree topology and reestablishes the link by activating the standby path.

Spanning-Tree Protocol operation is transparent to end stations, which are unaware whether they are connected to a single LAN segment or a switched LAN of multiple segments.

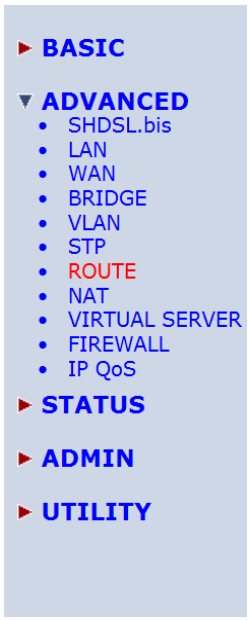
RSTP(Rapid Spanning Tree Protocol) defined in the IEEE 802.1w can be seen as an enhencement of the 802.1D standard. Most parameters have been left unchanged so users

familiar with 802.1D can quickly configure the new protocol. In most cases, RSTP performs better than STP.

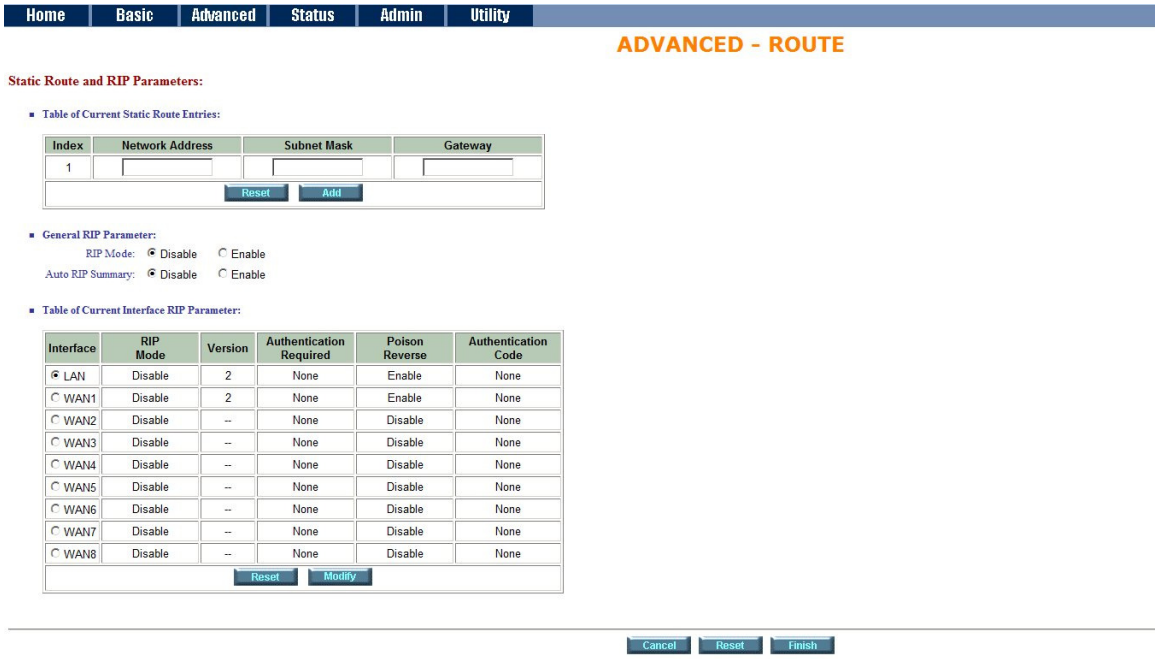
4.2.6 Route

If the Router is connected to more than one network, it may be necessary to set up a static route between them. A static route is a pre-determined pathway that network information must travel to reach a specific host or network.

With Dynamic Routing, you can enable the Router to automatically adjust to physical changes in the network's layout. The Router, using the RIP protocol, determines the network packets' route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other routers on the network.



Click Route to modify the routing information.



There are maximun 20 entries to set up the static router.

Press Add to add each entry. For example, there are 20 entries as follows:

Static Route and RIP Parameters:

- **Table of Current Static Route Entries:**

Index	Network Address	Subnet Mask	Gateway
1	192.168.1.1	255.255.255.0	192.168.0.254
2	192.168.2.2	255.255.255.0	192.168.0.254
3	192.168.3.3	255.255.255.0	192.168.0.254
4	192.168.4.4	255.255.255.0	192.168.0.254
5	192.168.5.5	255.255.255.0	192.168.0.254
6	192.168.6.6	255.255.255.0	192.168.0.254
7	192.168.7.7	255.255.255.0	192.168.0.254
8	192.168.8.8	255.255.255.0	192.168.0.254
9	192.168.9.9	255.255.255.0	192.168.0.254
10	192.168.10.10	255.255.255.0	192.168.0.254
11	192.168.11.11	255.255.255.0	192.168.0.254
12	192.168.12.12	255.255.255.0	192.168.0.254
13	192.168.13.13	255.255.255.0	192.168.0.254
14	192.168.14.14	255.255.255.0	192.168.0.254
15	192.168.15.15	255.255.255.0	192.168.0.254
16	192.168.16.16	255.255.255.0	192.168.0.254
17	192.168.17.17	255.255.255.0	192.168.0.254
18	192.168.18.18	255.255.255.0	192.168.0.254
19	192.168.19.19	255.255.255.0	192.168.0.254
20	192.168.20.20	255.255.255.0	192.168.0.254

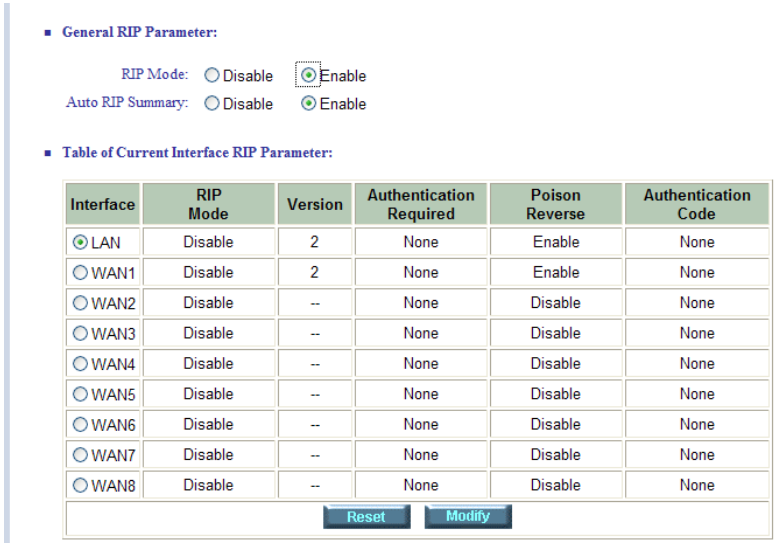
Reset Delete Modify

To modify the RIP (Routing information protocol) Parameters:

RIP Mode: Enable

Auto RIP Summary: Enable

Press Modify



■ General RIP Parameter:

RIP Mode: ○ Disable ◉ Enable

Auto RIP Summary: ○ Disable ◉ Enable

■ Table of Current Interface RIP Parameter:

Interface	RIP Mode	Version	Authentication Required	Poison Reverse	Authentication Code
◉ LAN	Disable	2	None	Enable	None
○ WAN1	Disable	2	None	Enable	None
○ WAN2	Disable	--	None	Disable	None
○ WAN3	Disable	--	None	Disable	None
○ WAN4	Disable	--	None	Disable	None
○ WAN5	Disable	--	None	Disable	None
○ WAN6	Disable	--	None	Disable	None
○ WAN7	Disable	--	None	Disable	None
○ WAN8	Disable	--	None	Disable	None

Reset Modify

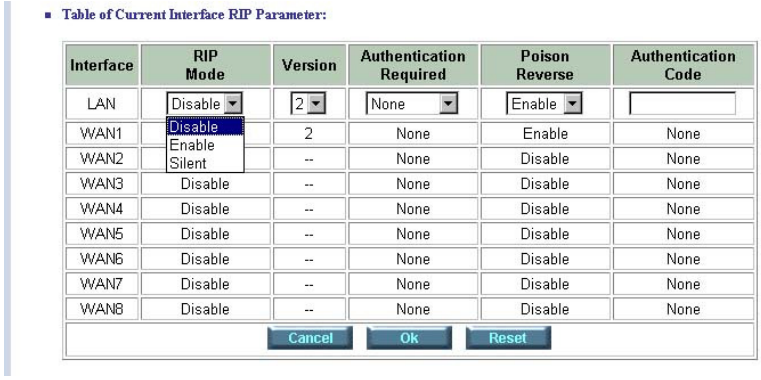
RIP Mode:

This parameter determines how the router handle RIP (Routing information protocol). RIP allows it to exchange routing information with other router.

Disable: The gateway does not participate in any RIP exchange with other routers.

Enable: The router broadcasts the routing table of the router on the LAN and incoporates RIP broadcast by other routers into it's routing table.

Silent: The router does not broadcast the routing table, but it accepts RIP broadcast packets that it receives.



■ Table of Current Interface RIP Parameter:

Interface	RIP Mode	Version	Authentication Required	Poison Reverse	Authentication Code
LAN	Disable	2	None	Enable	
WAN1	Disable Enable Silent	2	None	Enable	None
WAN2	Disable	--	None	Disable	None
WAN3	Disable	--	None	Disable	None
WAN4	Disable	--	None	Disable	None
WAN5	Disable	--	None	Disable	None
WAN6	Disable	--	None	Disable	None
WAN7	Disable	--	None	Disable	None
WAN8	Disable	--	None	Disable	None

Cancel Ok Reset

RIP Version:

It determines the format and broadcasting method of any RIP transmissions by the gateway.

RIP v1: it only sends RIP v1 messages only.

RIP v2: it sends RIP v2 messages in multicast and broadcast format.

■ Table of Current Interface RIP Parameter:

Interface	RIP Mode	Version	Authentication Required	Poison Reverse	Authentication Code
LAN	Disable	2 (1, 2)	None	Enable	
WAN1	Disable	--	None	Enable	None
WAN2	Disable	--	None	Disable	None
WAN3	Disable	--	None	Disable	None
WAN4	Disable	--	None	Disable	None
WAN5	Disable	--	None	Disable	None
WAN6	Disable	--	None	Disable	None
WAN7	Disable	--	None	Disable	None
WAN8	Disable	--	None	Disable	None

Cancel Ok Reset

Authentication required:

None: for RIP, there is no need of authentication code.

Password: the RIP is protected by password/authentication code.

MD5: The RIP will be decoded by MD5 then protected by password/authentication code.

■ Table of Current Interface RIP Parameter:

Interface	RIP Mode	Version	Authentication Required	Poison Reverse	Authentication Code
LAN	Disable	2	None (None, Password, MD5)	Enable	
WAN1	Disable	2		Enable	None
WAN2	Disable	--		Disable	None
WAN3	Disable	--	None	Disable	None
WAN4	Disable	--	None	Disable	None
WAN5	Disable	--	None	Disable	None
WAN6	Disable	--	None	Disable	None
WAN7	Disable	--	None	Disable	None
WAN8	Disable	--	None	Disable	None

Cancel Ok Reset

Poison Reserve:

Poison Reserve is for the purpose of promptly broadcast or multicast the RIP while the route is changed. (ex shuting down one of the routers in routing table)

Enable: the gateway will actively broadcast or multicast the information.

Disable: the gateway will not broadcast or multicast the information.

■ Table of Current Interface RIP Parameter:

Interface	RIP Mode	Version	Authentication Required	Poison Reverse	Authentication Code
LAN	Disable	2	None	Enable (Disable, Enable)	
WAN1	Disable	2	None		None
WAN2	Disable	--	None		None
WAN3	Disable	--	None	Disable	None
WAN4	Disable	--	None	Disable	None
WAN5	Disable	--	None	Disable	None
WAN6	Disable	--	None	Disable	None
WAN7	Disable	--	None	Disable	None
WAN8	Disable	--	None	Disable	None

Cancel Ok Reset

Authentication code:

You can set up a authentication code here.

After modifying the RIP parameters, press finish.

The screen will prompt the modified parameter. Check the parameters and perss Restart to restart the router or press Continue to setup another parameters.

4.2.7 NAT/DMZ

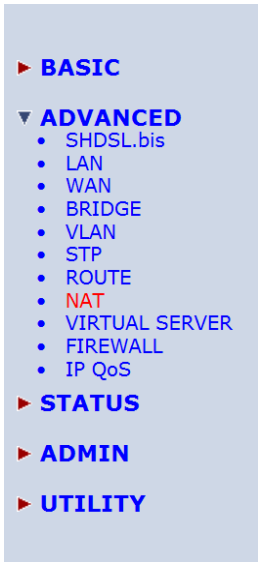
NAT *(Network Address Translation) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and reverse the global IP addresses of incoming packets back into local IP addresses. This ensure security since each outgoing or incoming request must go through a translation process, that also offers the opportunity to qualify or authenticate the request or match it to a previous request. NAT also conserves on the number of global IP addresses that a company needs and lets the company to use a single IP address of its communication in the Internet world.*

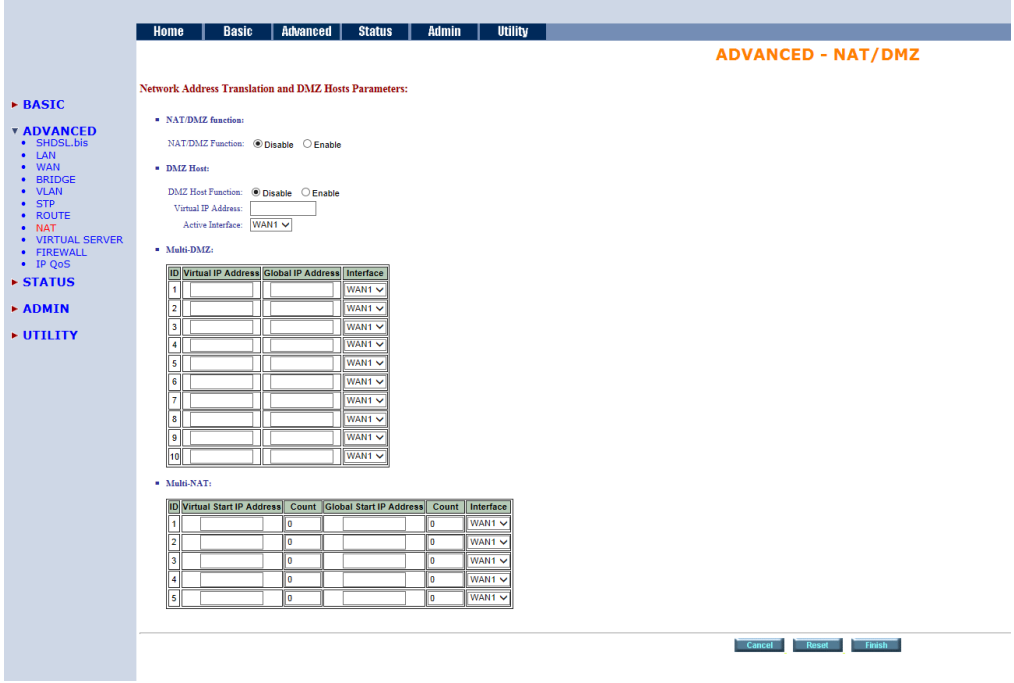
DMZ *(Demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company private network and the outside public network. It prevents outside users from getting direct access to a server that has company private data.*

In a typical DMZ configuration for an enterprise, a separate computer or host receives requests from users within the private network to access via Web sites or other companies accessible on the public network. The DMZ host then initiates sessions for these requests to the public network. However, the DMZ host is not able to initiate a session back into the private network. It can only forward packets that have already been requested.

Users of the public network outside the company can access only the DMZ host. The DMZ may typically also have the company's Web pages so these could serve the outside world. However, the DMZ provides access to no other company data. In the event that an outside user penetrated the DMZ host's security, the Web pages might be corrupted, but no other company information would be exposed.

Press NAT to setup the parameters.





If you want to enable the NAT/DMZ functions, click Enable. The IP address assigned to the WAN will enable DMZ function for the virtual IP address.

4.2.7.1 Multi-DMZ

Some users have two or more global IP addresses assigned by ISP can use multi DMZ. The table is for mapping of global IP address and virtual IP address.

4.2.7.2 Mutli-NAT

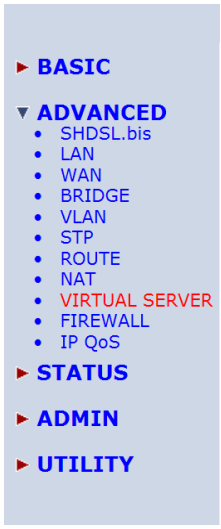
Some of the virtual IP addresses (eg: 192.168.0.10 ~ 192.168.0.50) collectively use two of the global IP addresses (eg: 69.210.1.9 and 69.210.1.10). The Multi-NAT table will be setup as;
Virtual Start IP Address: 192.168.0.10
Count: 40
Global Start IP Address: 69.210.1.9
Count: 2
Press Finish to continue to review.

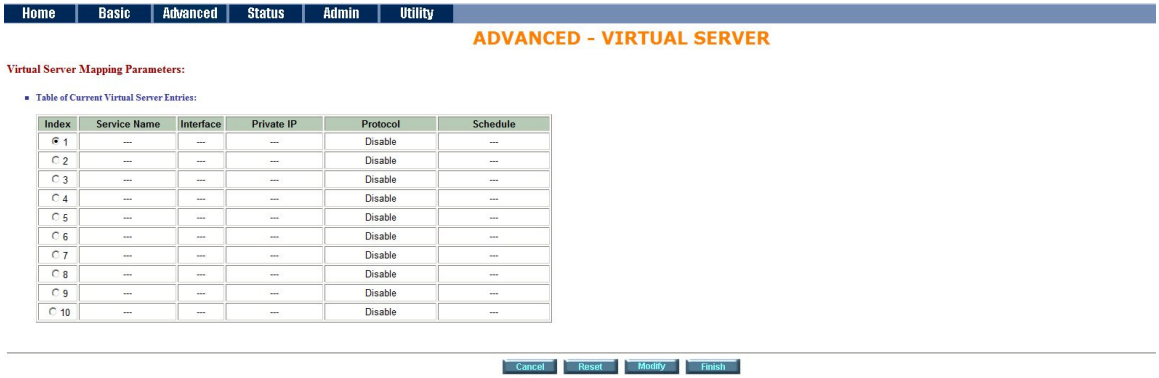
The screen will prompt the parameters that will be written in NVRAM. Check the parameters before writing in NVRAM. Press Restart to restart the router working with new parameters or Continue to configure another parameter.

4.2.8 Virtual Server

This section guides you to configure Virtual Servers.

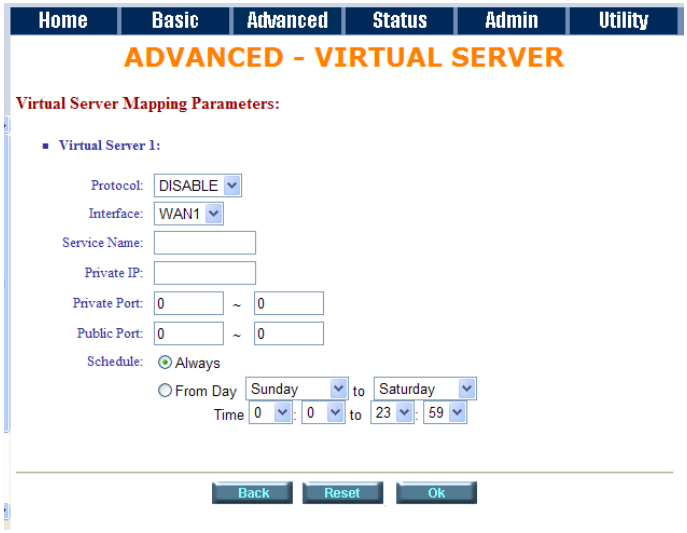
Click Virtual Server to configure the parameters.





Up to ten virtual servers index form 1 to 10 can been configured.

Press Modify to modify index 1.



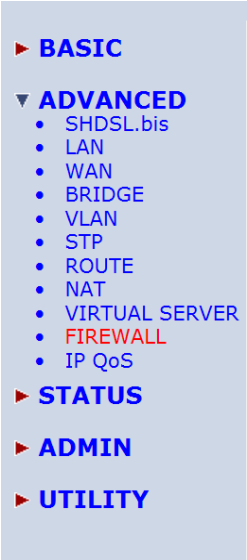
Type the necessary parameters and then click OK.

Press Restart to restart the router or press Continue to setup another function.

For example:
You can setup the router as Index 1, protocol TCP, interface WAN1, service name test1, private IP 192.168.0.2, private port 80, public port 80, schedule from Day Monday to Friday and time 8:0 to 16:0 and index 2, protocol UDP, interface WAN1, service name test2, private IP 192.168.0.3, private port 25, public port 25, schedule always.

Home
Basic
Advanced
Status
Admin
Utility
ADVANCED - VIRTUAL SERVER
Virtual Server Mapping Parameters:
Table of Current Virtual Server Entries:
Index | Service Name | Interface | Private IP | Protocol | Schedule
1 | test1 | WAN1 | 192.168.0.2 | TCP 80/80 | Mon.-Fri. 8:0-16:0
2 | test2 | WAN1 | 192.168.0.3 | UDP 25/25 | Always
3 | --- | --- | --- | Disable | ---
4 | --- | --- | --- | Disable | ---
5 | --- | --- | --- | Disable | ---
6 | --- | --- | --- | Disable | ---
7 | --- | --- | --- | Disable | ---
8 | --- | --- | --- | Disable | ---
9 | --- | --- | --- | Disable | ---
10 | --- | --- | --- | Disable | ---
Cancel
Reset
Modify
Finish

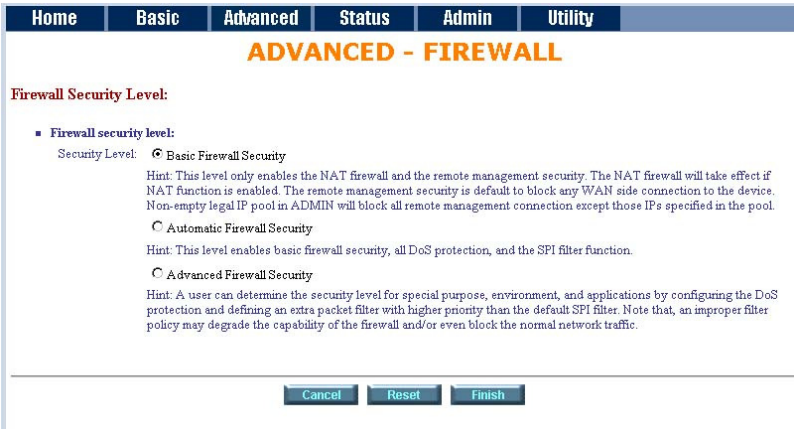
4.2.9 Firewall



A firewall is a set of related programs that protects the resources of a private network from other networks. It prevents hackers to access your private data resource.

There are three security levels: **Basic firewall security**, **Automatic firewall security** and **advanced firewall security**.

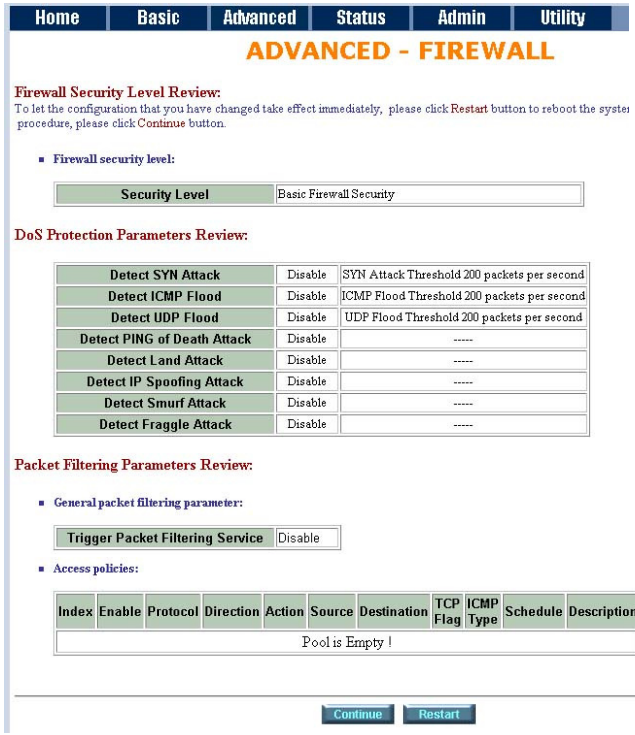
4.2.9.1 Basic Firewall Security


Home
Basic
Advanced
Status
Admin
Utility
ADVANCED - FIREWALL
Firewall Security Level:
Firewall security level:
Security Level:
Basic Firewall Security
Hint: This level only enables the NAT firewall and the remote management security. The NAT firewall will take effect if NAT function is enabled. The remote management security is default to block any WAN side connection to the device. Non-empty legal IP pool in ADMIN will block all remote management connection except those IPs specified in the pool.
Automatic Firewall Security
Hint: This level enables basic firewall security, all DoS protection, and the SPI filter function.
Advanced Firewall Security
Hint: A user can determine the security level for special purpose, environment, and applications by configuring the DoS protection and defining an extra packet filter with higher priority than the default SPI filter. Note that, an improper filter policy may degrade the capability of the firewall and/or even block the normal network traffic.
Cancel
Reset
Finish

Click Basic Firewall Security.

This level only enables the NAT firewall and the remote management security. The NAT firewall will take effect when NAT function is enabled. The remote management security by default will block any WAN side connection to the device. Non-empty legal IP pool in ADMIN will block all remote management connection except those IPs specified in the pool.

Press Finish to finish setting of firewall and review the parameters.

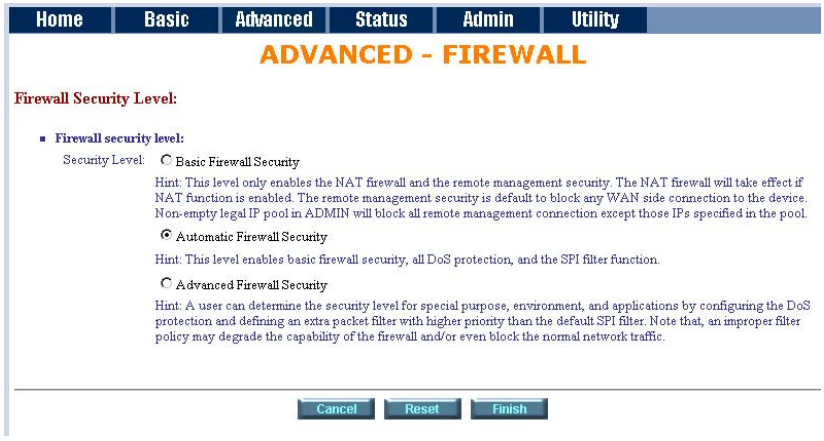


The screen will prompt the parameters to be recorded in NVRAM. Please Check these parameters.

Press Restart to restart the router or press Continue to setup another function.

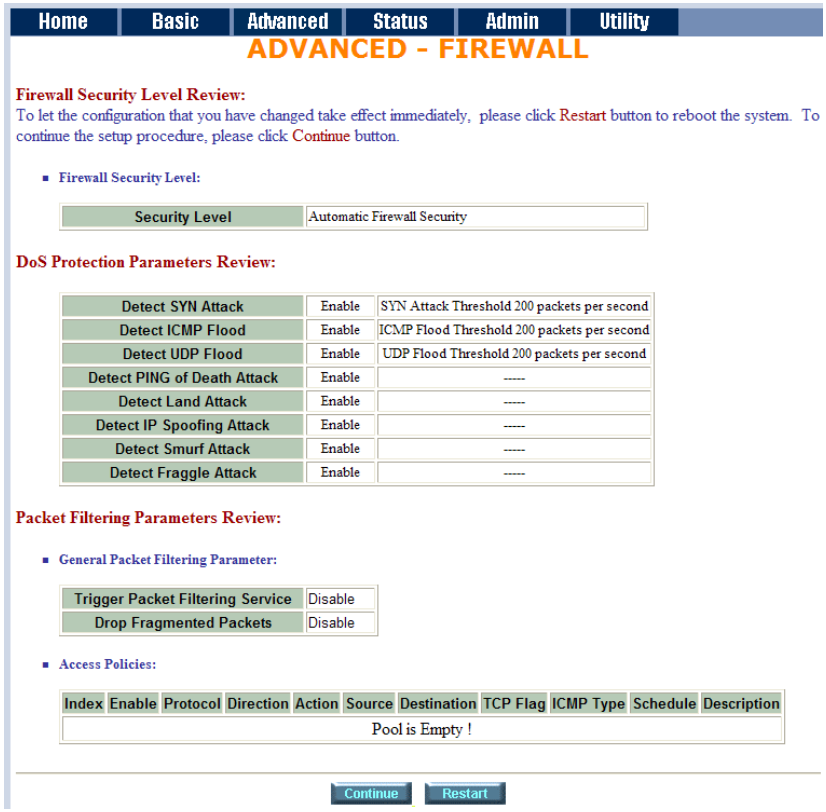
4.2.9.2 Automatic Firewall Security

Click Automatic Firewall Security.


Home
Basic
Advanced
Status
Admin
Utility
ADVANCED - FIREWALL
Firewall Security Level:
Firewall security level:
Security Level:
Basic Firewall Security
Hint: This level only enables the NAT firewall and the remote management security. The NAT firewall will take effect if NAT function is enabled. The remote management security is default to block any WAN side connection to the device. Non-empty legal IP pool in ADMIN will block all remote management connection except those IPs specified in the pool.
Automatic Firewall Security
Hint: This level enables basic firewall security, all DoS protection, and the SPI filter function.
Advanced Firewall Security
Hint: A user can determine the security level for special purpose, environment, and applications by configuring the DoS protection and defining an extra packet filter with higher priority than the default SPI filter. Note that, an improper filter policy may degrade the capability of the firewall and/or even block the normal network traffic.
Cancel
Reset
Finish

This level enables basic firewall security, all DoS protection and the SPI filter function.

Press Finish to complete setting firewall.



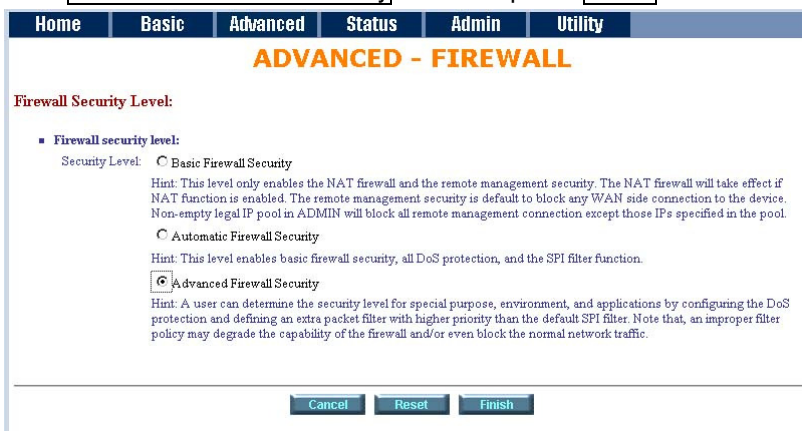
The screen will prompt the parameters, which will be written in NVRAM. Please check these parameters.

Press Restart to restart the router or press Continue to setup another function.

User can determine the security level for special purpose, environment, and applications by configuring the DoS protection and defining an extra packet filter. Please note that an improper filter policy may degrade the capability of the firewall and/or even block the normal network traffic.

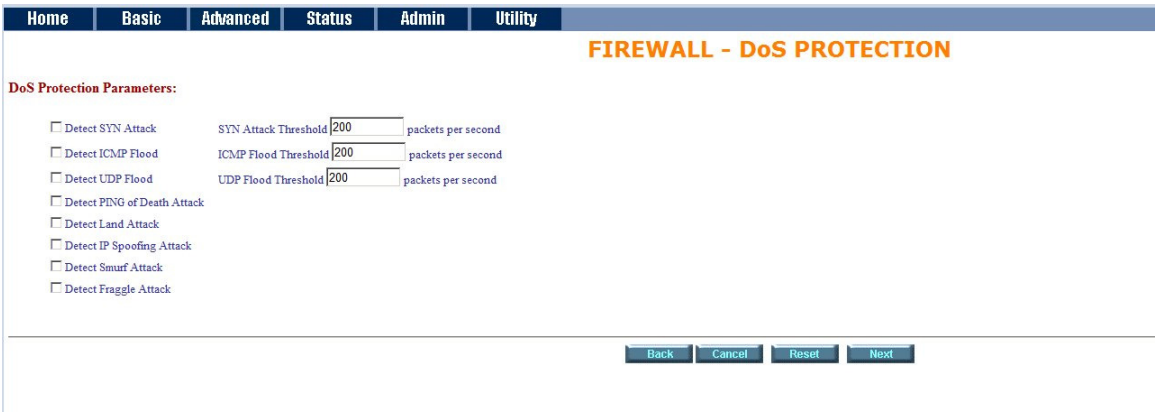
4.2.9.3 Advanced Firewall Security

Click Advanced Firewall Security and then press Finish.


Home
Basic
Advanced
Status
Admin
Utility
ADVANCED - FIREWALL
Firewall Security Level:
Firewall security level:
Security Level:
Basic Firewall Security
Hint: This level only enables the NAT firewall and the remote management security. The NAT firewall will take effect if NAT function is enabled. The remote management security is default to block any WAN side connection to the device. Non-empty legal IP pool in ADMIN will block all remote management connection except those IPs specified in the pool.
Automatic Firewall Security
Hint: This level enables basic firewall security, all DoS protection, and the SPI filter function.
Advanced Firewall Security
Hint: A user can determine the security level for special purpose, environment, and applications by configuring the DoS protection and defining an extra packet filter with higher priority than the default SPI filter. Note that, an improper filter policy may degrade the capability of the firewall and/or even block the normal network traffic.
Cancel
Reset
Finish

A user can determine the security level for special purpose, environment and applications by configuring the DoS protection and defining an extra packet filter. Please notice that an improper filter policy may degrade the capability of the firewall and even block the normal network traffic.

It can set up the DoS protection parameters



SYN flood: A SYN flood is a form of denial-of-service attack, attempts to slow your network by requesting new connections but not completing the process to open the connection. Once the buffer for these pending connections is full a server will not accept any more connections and will be unresponsive.

ICMP flood: A sender transmits a volume of ICMP request packets to cause all CPU resources to be consumed serving the phony requests.

UDP Flood: A UDP flood attack is a denial-of-service (DoS) attack using the User Datagram Protocol(UDP). A sender transmits a volume of requests for UDP diagnostic services which cause all CPU resources to be consumed serving the phony requests.

Ping of Death: A ping of death (abbreviated ”POD”) attack attempts to crash your system by sending a fragmented packet, when reconstructed is larger than the maximum allowable size.

Land attack: A land attack is an attempt to slow your network down by sending a packet with identical source and destination addresses originating from your network.

IP Spoofing: IP Spoofing is a method of masking the identity of an intrusion by making it appeared that the traffic came from a different computer. This is used by intruders to keep their anonymity and can be used in a Denial of Service attack.

Smurf attack: The Smurf attack is a way of generating a lot of computer network traffic to a victim host. That is a type of denial-of-service attack. A Smurf attack involves two systems. The attacker sends a packet containing an ICMP echo request (ping) to the network address of one system. This system is known as the amplifier. The return address of the ping has been faked (spoofed) to appear to come from a machine on another network (the victim). The victim is then flooded with responses to the ping. As many responses are generated for only one attack, the attacker is able use many amplifiers on the same victim.

Fraggle attack: A Fraggle attack is a type of denial-of-service attack where an attacker sends a large amount of UDP echo traffic to IP broadcast addresses, all of it having a fake source address. This is a simple rewrite of the smurf attack code.

For SYN attack, ICMP flood and UDP flood, they can set up the threshold of packets number per second. The default values are 200 packets per second. If everything is working properly, you probably do not need to change the threshold setting as the default threshold values. Reduce the

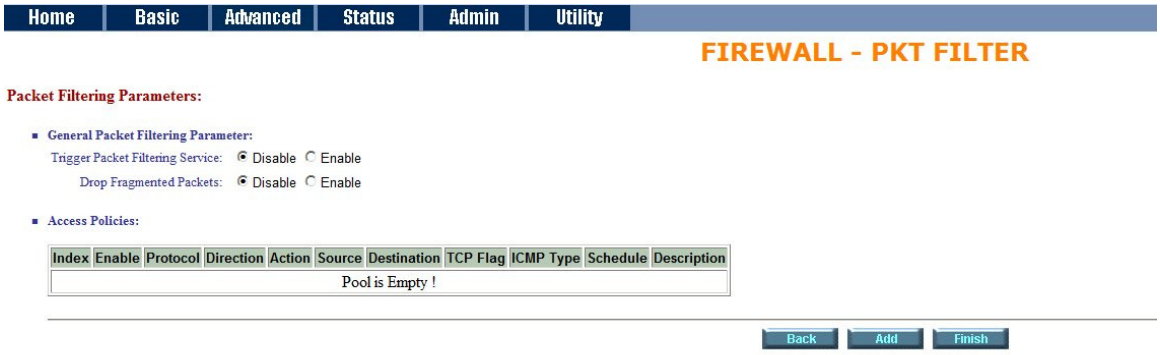
threshold values if your network is slower than average.

Traditional firewall is stateless meaning they have no memory of the connections of data or packets that pass through them. Such IP filtering firewalls simply examine header information in each packet and attempt to match it to a set of define rule. If the firewall finds a match, the prescribe action is taken. If no match is found, the packet is accepted into the network, or dropped, depending on the firewall configuration.

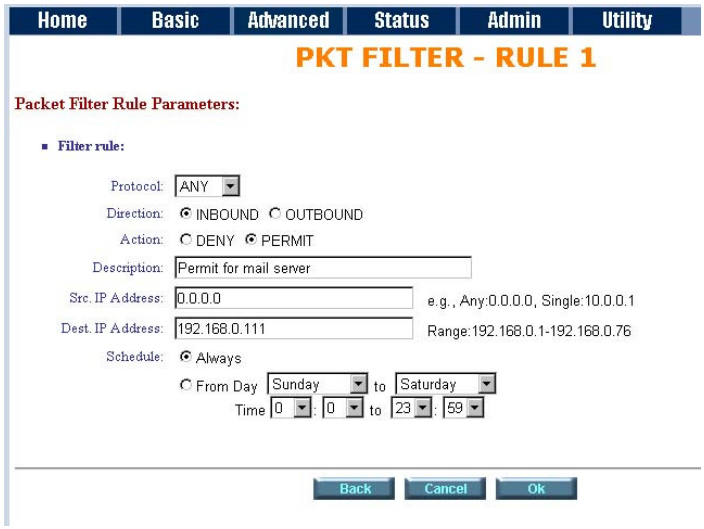
Packet filter

Click Next can set up the packet filtering parameters.

If you want to configure the Packet Filtering Parameters, choose **Enable** and press Add.



It can setup the packet filter rule parameters:



Select the Protocol and configure the parameter.

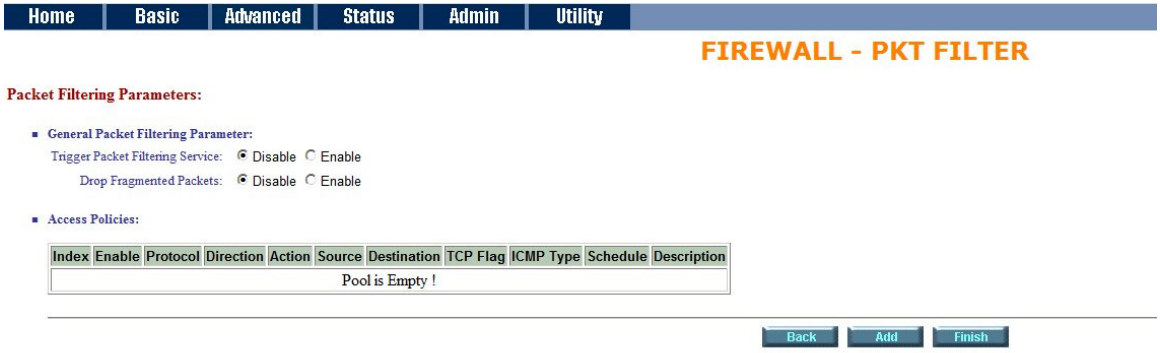
Protocol: ANY, TCP, UDP, ICMP, GRE, RSVP, ESP and AH.(ANY means all protocol)

TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
GRE	Generic Routing Encapsulation
RSVP	Resource Reservation Protocol
ESP	Encapsulating Security Payload
AH	Authentication Header

Direction: INBOUND (from WAN to LAN) or OUTBOUND (from LAN to WAN)
Action: DENY(block) or PERMIT(allow)
Description: Type a description for your customized service..
Src. IP Address: The source addresses or ranges of addresses to which this packet filter rule applies. (Address 0.0.0.0 is equivalent Any)
Dest. IP Address: The destination addresses or ranges of addresses to which this packet filter rule applies. (Address 0.0.0.0 is equivalent Any)
Schedule: Select everyday (always) or the day(s) of the week to apply the rule. Enter the start and end times in the hour-minute format to apply the rule.

For example, If you want to ban all of the protocol from the IP (e.g.: 200.1.1.1) to access the all PCs (e.g.: 192.168.0.2 ~ 192.168.0.50) in the LAN, key in the parameter as:

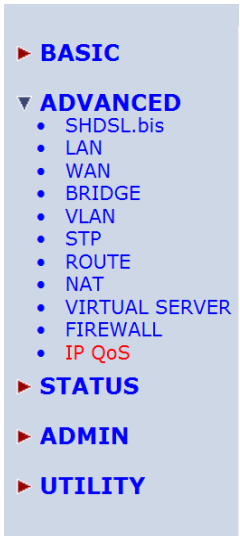
Protocol: ANY
Direction: INBOUND (INBOUND is from WAN)
Action: DENY
Description: Hacker
Src. IP Address: 200.1.1.1
Dest. IP Address: 192.168.0.2-192.168.0.50
Schedule: You can set always or any time range which you want
Press OK to finish.

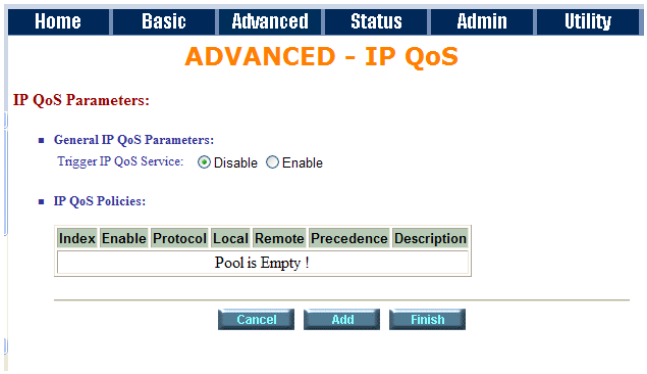


The screen will prompt the configured parameters.
Click Enable on Trigger Packet Filtering Service item, to active the packet filtering service.
Click Enable on Drop Fragmented Packets item, to active the drop fragmented packets operation.
You can modify or delete the access policies by click Modify or Delete command.

4.2.10 IP QoS

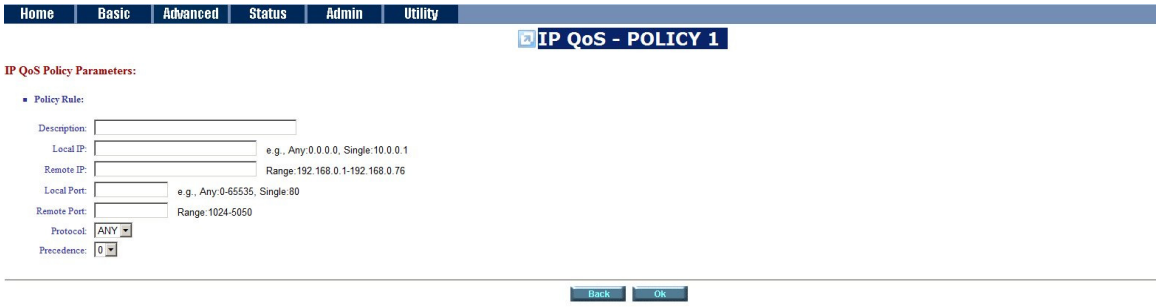
IP QoS is a function to decide the priorities of setting IPs to transfer packets under the situation of overloading bandwidth.





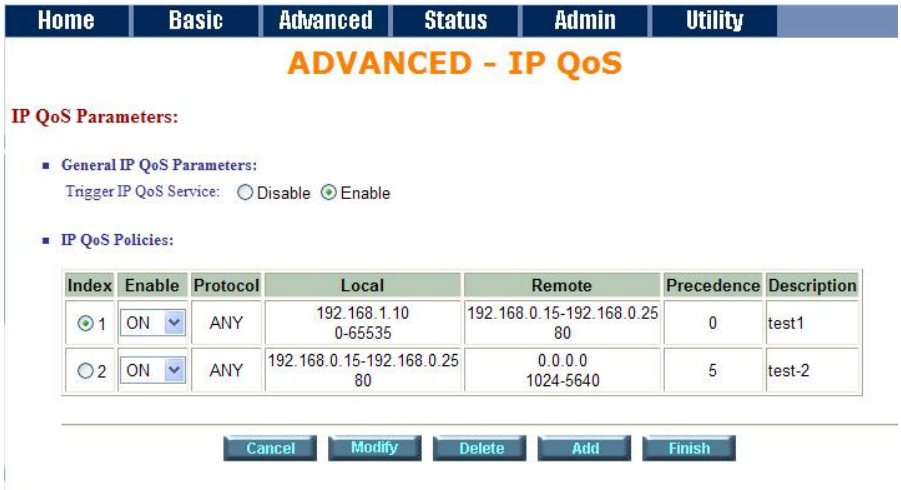
Click Enable at item Trigger IP QoS Service in General IP QoS Parameter, which will turn on this IP QoS function.

Click Add in the bottom of web page to begin a new entry in IP QoS Policy table.



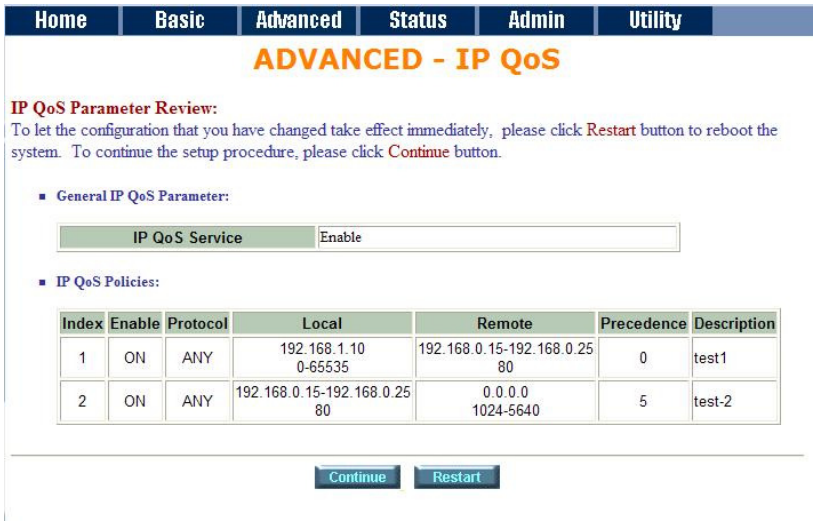
Description: A brief statement describe this policy
Local IP: type IP address of local host in prioritized session.
Remote IP: type IP address of remote host in prioritized session.
Local Port: type the service port number of local host in prioritized session.
Remote Port: type the service port number of remote host in prioritized session.
Protocol: identify the transportation layer protocol type you want to prioritize, ex: **TCP** or **UDP**. The default is **ANY**.
Precedence: type the session's prioritized level you classify, "**0**" is lowest priority, "**5**" is highest priority.

Click OK when all parameters are finish.



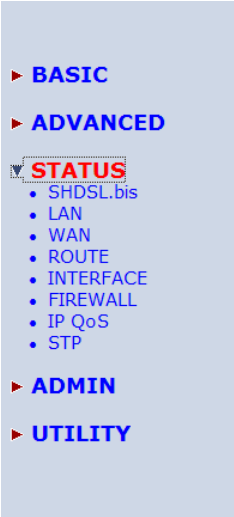
You can modify or delete the policies by click Modify or Delete command

Click Finish can make a review for all IP QoS parameter



To let the IP QoS configuration you have changed and want those take effect immediately, please click Restart button to reboot the system. To continue the setup procedure, please click Continue button.

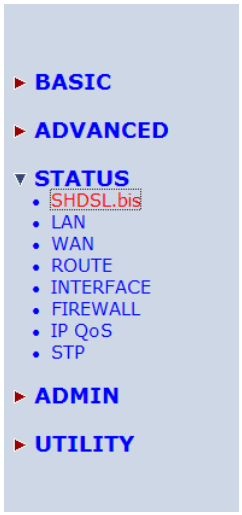
4.3 Status

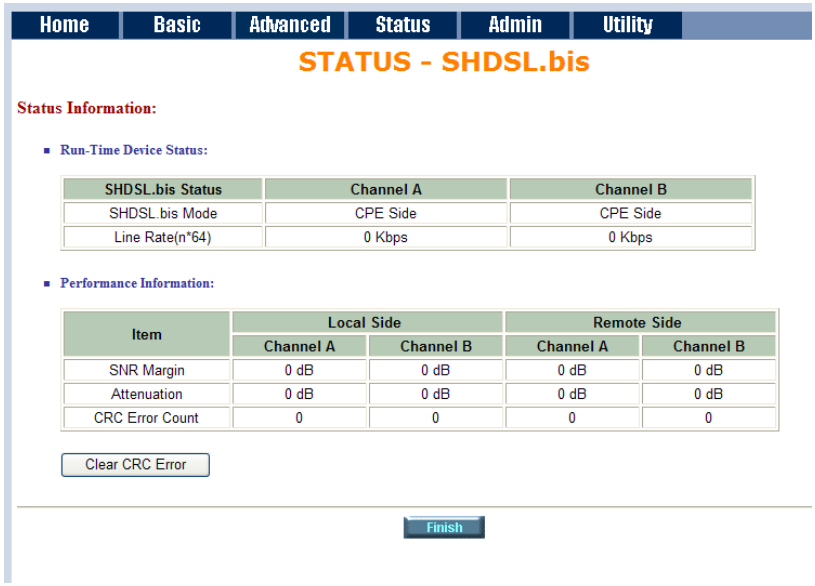


On STATUS item, you can monitor the following:

SHDSL.bis	Mode, Line rate and Performance information including SNR margin, atteunation and CRC error count.
LAN	IP type, MAC address, IP address, Subnet mask and DHCP client table: Type, IP address and MAC address.
WAN	WAN interface information. 8 WAN interface including IP address, Subnet Mask, VPI/VCI, Encapsulation, Protocol and Flag.
ROUTE	IP routing table including Flags, Destination IP/Netmask.Gateway, Interface and Portname.
INTERFACE	LAN and WAN statistics information.
FIREWALL	Current DoS protection status and dropped packets statistics.
IP QoS	Show IP QoS statistics on LAN interface
STP	STP information include Bridge parameter and Ports Parameter

4.3.1 SHDSL.bis

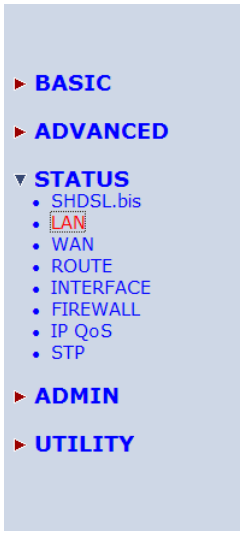




The status information shows this is a 4-wire model which has both channel A and B. If the router has connected to a remote side, it can also show the performance information of remote side.
It the router is 2-wire model, you will not see any information on channel B.

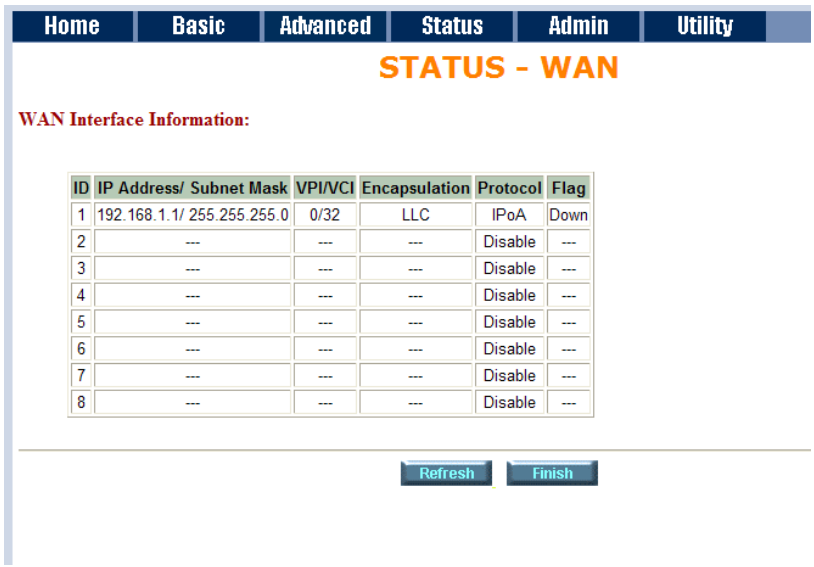
Click Clear CRC Error can clear the CRC error count.

4.3.2 LAN



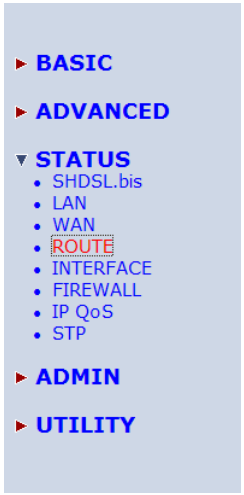
This information shows the LAN interface status and DHCP client table.

4.3.3 WAN

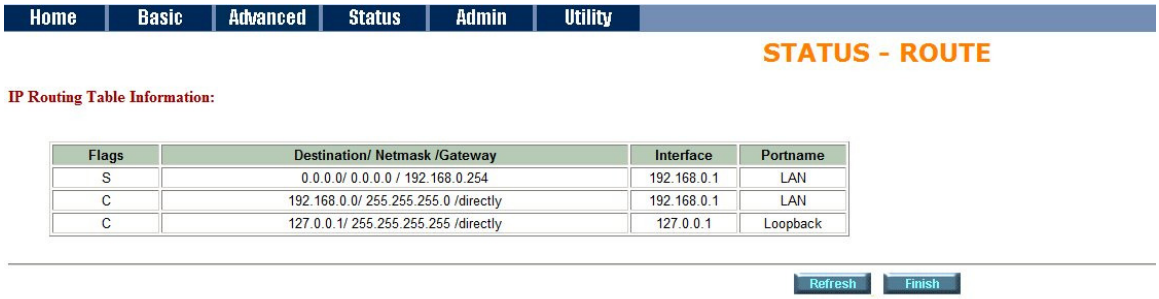

Home
Basic
Advanced
Status
Admin
Utility
STATUS - WAN
WAN Interface Information:
ID | IP Address/ Subnet Mask | VPI/VCI | Encapsulation | Protocol | Flag
1 | 192.168.1.1/ 255.255.255.0 | 0/32 | LLC | IPoA | Down
2 | --- | --- | --- | Disable | ---
3 | --- | --- | --- | Disable | ---
4 | --- | --- | --- | Disable | ---
5 | --- | --- | --- | Disable | ---
6 | --- | --- | --- | Disable | ---
7 | --- | --- | --- | Disable | ---
8 | --- | --- | --- | Disable | ---
Refresh
Finish

This information shows the status of all eight WAN interfaces.

4.3.4 ROUTE

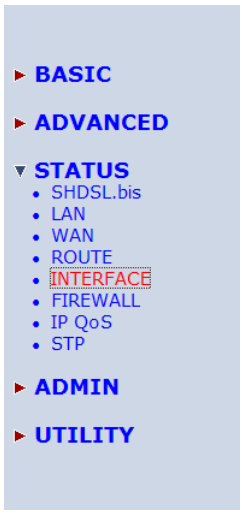


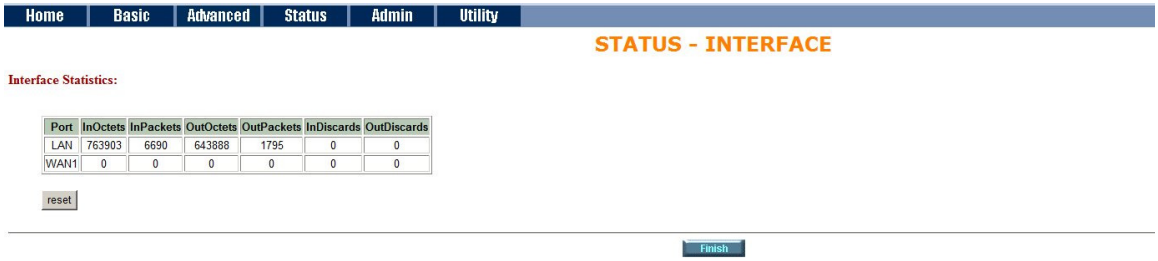
Routing tables contain a list of IP addresses. Each IP address identifies a remote router (or other network gateway) that the local router is configured to recognize. For each IP address, the routing table additionally stores a network mask and other data that specifies the destination IP address ranges that remote device will accept.



This information shows the IP routing table.

4.3.5 INTERFACE



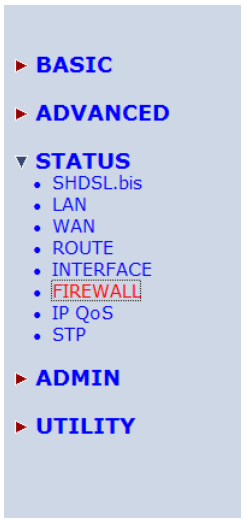


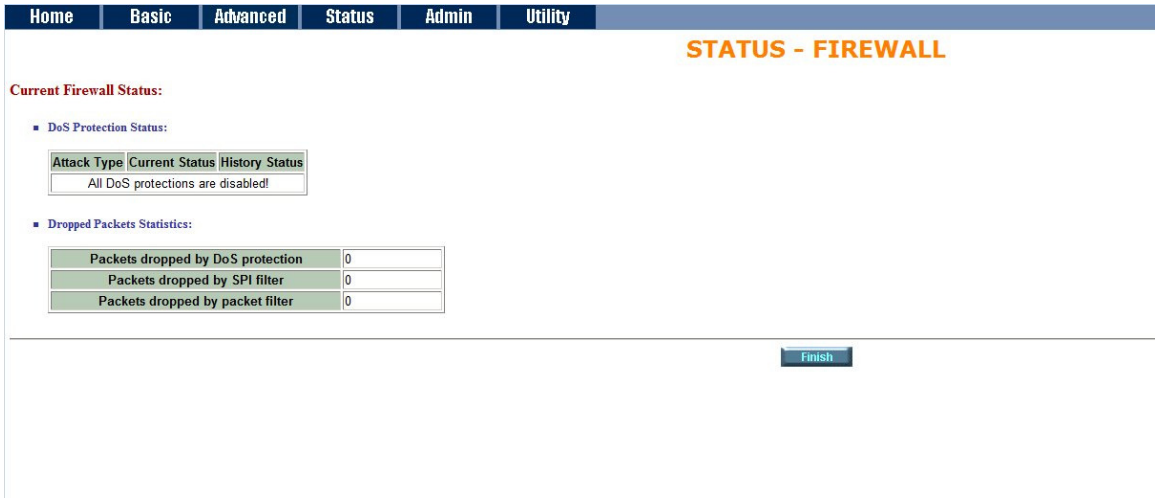
This table shows the interface statistics.

Octet is a group of 8 bits, often referred to as a byte.
Packet is a formatted block of data carried by a packet mode computer networks, often referred to the IP packet.

InOctets	The field shows the number of received bytes on this port
InPactets	The field shows the number of received packets on this port
OutOctets	The field shows the number of transmitted bytes on this port
OutPactets	The field shows the number of transmitted packets on this port
InDiscards	The field shows the discarded number of received packets on this port
OutDiscards	The field shows the discarded number of transmitted packets on this port

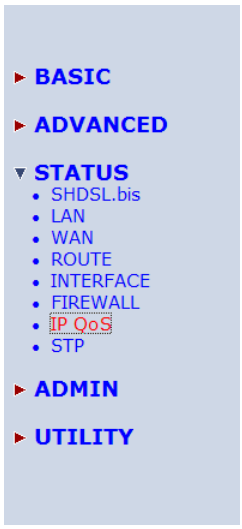
4.3.6 FIREWALL

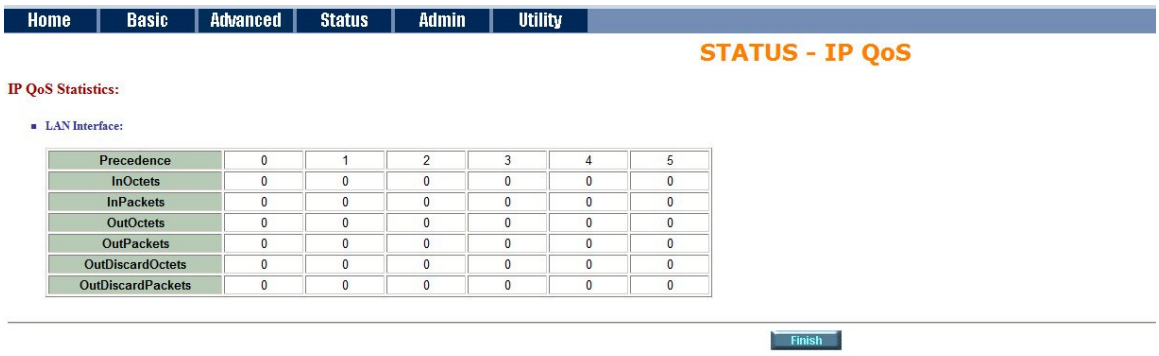




This information shows firewall status: DoS protection and dropped packets statistics.

4.3.7 IP QoS



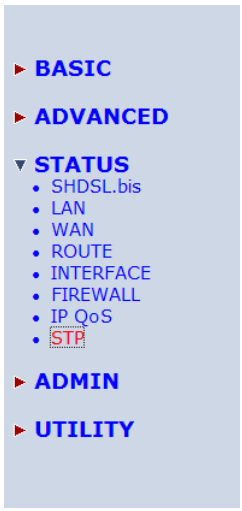


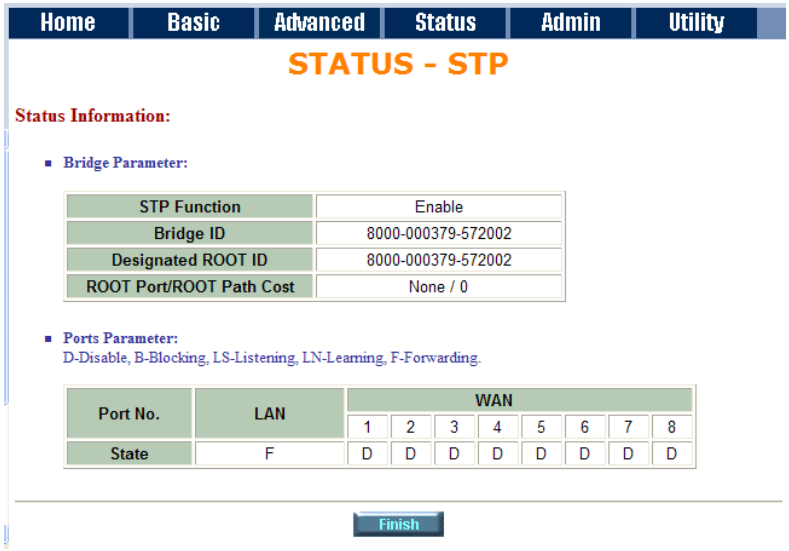
This information shows IP QoS statistics.

Octet is a group of 8 bits, often referred to as a byte.
Packet is a formatted block of data carried by a packet mode computer networks, often referred to the IP packet.

InOctets	The field shows the number of received bytes on this port
InPactets	The field shows the number of received packets on this port
OutOctets	The field shows the number of transmitted bytes on this port
OutPactets	The field shows the number of transmitted packets on this port
OutDiscardsOctets	The field shows the discarded number of transmitted bytes on this port
OutDiscardsPackets	The field shows the discarded number of transmitted packets on this port

4.3.8 STP





This information shows the STP parameter:

The bridge parameters have:

Bridge ID: The bridge ID of a configuration message is an 8-byte field. The six low order bytes are the MAC address of the switch. The high order two-byte (unsigned 16-bit integer) field is the bridge priority number.

Designated Root ID: The unique Bridge Identifier of the Bridge assumed to be the Root, this parameter is used as the value of the Root Identifier parameter in all CBPDUs transmitted by the Bridge.

Root Port: Identifies the Port through which the path to the Root is established, and is not significant when the Bridge is the Root and is set to zero. It is the Port Identifier of the Port that offers the lowest Cost Path to the Root

Root Path Cost: The Cost of the Path to the Root from this Bridge, this is equal to the sum of the values of the Designated Cost and Path Cost parameters held for the Root Port. When the Bridge is the Root, this parameter is zero.

The ports parameters have:

Learning: This is when the modem creates a switching table that will map MAC addresses to port number.

Listening: This is when the modem processes BPDU's that allow it to determine the network topology.

Forwarding: When a port receives or sends data. In other words, this is operating normally.

Disabled: This is when the network administrator has disabled the port.

Blocking: this means the port was blocked to stop a looping condition.

4.4 Administration

This session introduces security and simple network management protocol (SNMP) and time synchronous.

4.4.1 Security

For system secutiry, please change the default user name and password in the first setup otherwise unauthorized persons can access the router and change the parameters.
There are three ways to configure the router: Web browser, telnet and serial console.

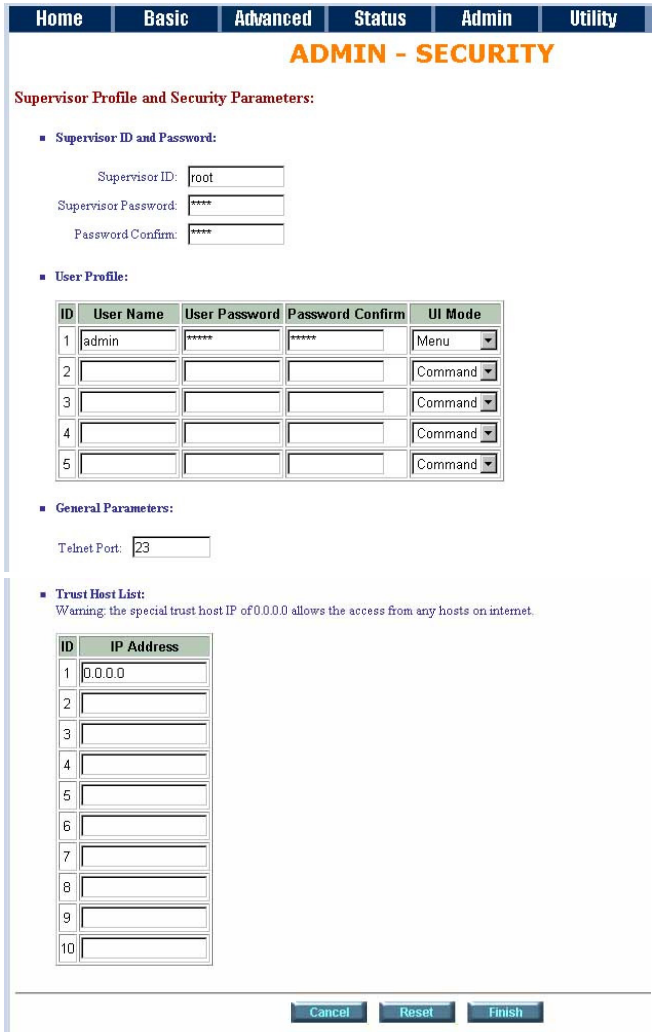
Press **Security** to setup the parameters.

For greater security, change the Supervisor ID and password for the router. If you don't set them, all users on your network can be able to access the router using the default Supervisor IP and Supervisor Password is "***root***".

You can authorize five legal users to access the router via telnet or console only. There are two UI modes: **menu driven mode** and **line command mode** to configure the router. There are two UI modes, menu and command mode for telnet or console mode to setup the Router. The menu is meaning menu driven interface mode and Command is meaning line command mode. We will not discuss command mode in this manual.

The default user name on and Password are *"**admin**"*.

Legal address pool will setup the legal IP addresses from which authorized person can configure the router. This is the more secure function for network administrator to setup the legal address of configuration.



This is the default supervisor ID and password is "***root***". It is highly recommended that you change these for security purpose.
Supervisor ID: Type the new ID
Supervisor Password: Type the existing password ("***root***" is the default password when shipped)
Password Confirm: Retype your new password for confirmation.

Telnet Port: For Telnet, you may change the default service port by typing the new port number. If you change the default port number then you will have to let user who wish to use the service know the new port number. The default value is 23.

On trust host list, configured 0.0.0.0 will allow all hosts on Internet or LAN to access the router.

Leaving blank of trust host list will cause blocking all PC from WAN to access the router. On the other hand, only PC in LAN can access the router.

If you type the excact IP address in the filed, only the host on this listing can access to the router.
Click Finish to finish the setting.

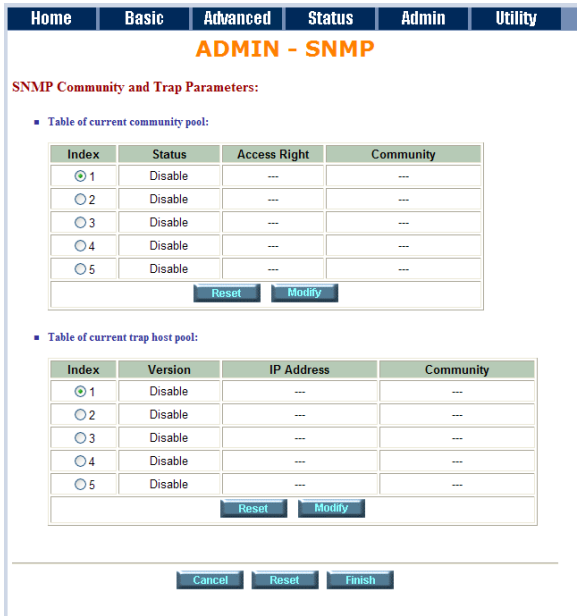
The browser will prompt the all configured parameters and check it before writing into NVRAM. Press Restart to restart the gateway working with the new parameters and press Continue to setup other parameters.

4.4.2 SNMP

Simple Network Management Protocol (SNMP) provides for the exchange of messages between a network management client and a network management agent for remote management of network nodes. These messages contain requests to get and set variables that exist in network nodes in order to obtain statistics, set configuration parameters, and monitor network events. SNMP communications can occur over the LAN or WAN connection.

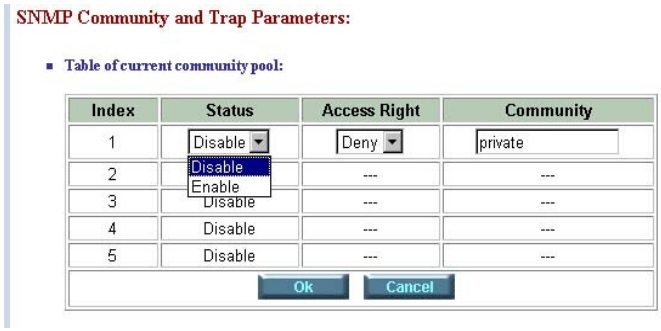
The router can generate SNMP traps to indicate alarm conditions, and it relies on SNMP community strings to implement SNMP security.
This router support both MIB I and MIB II.

Click SNMP to configure the parameters.

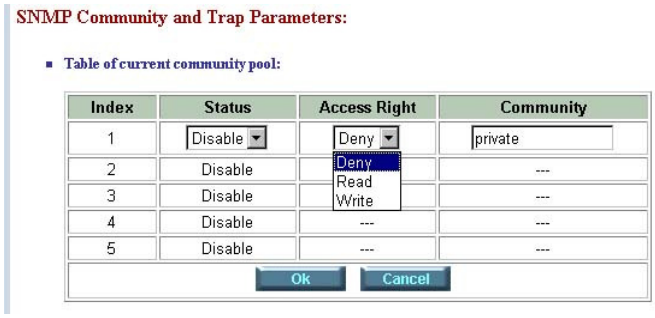


4.4.2.1 Community pool

Press Modify to modify the community pool. You can setup the access authority.



SNMP **Status**: Enable



Access Right: Deny for deny all access
Read for access read only
Write for access read and write.

Community: it serves as password for access right.
After configuring the community pool, press OK.

4.4.2.2 Trap host pool

SNMP trap is an informational message sent from an SNMP agent to a manager. Click Modify to modify the trap host pool.

Version: select version for trap host. (Version 1 is for SNMPv1; Version 2 for SNMPv2).
IP Address: type the trap host IP address
Community: type the community password. The community is setup in community pool.

Press OK to finish the setup.

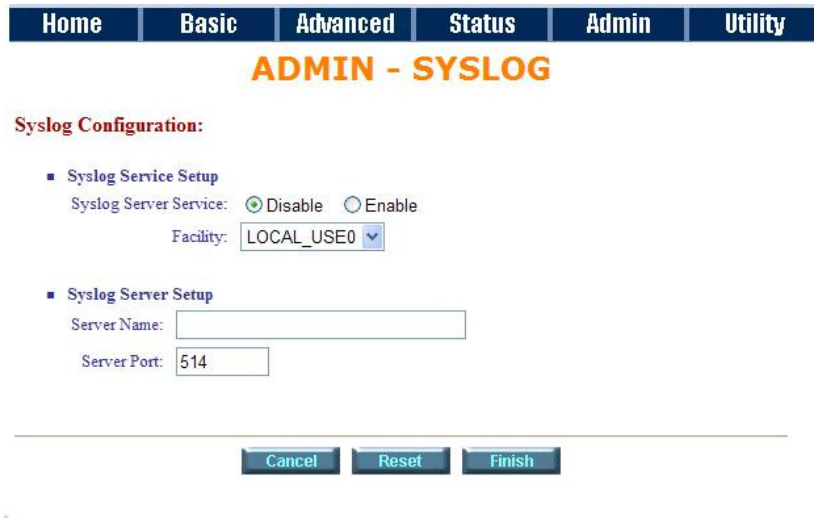
The browser will prompt the configured parameters and check it before writing into NVRAM.

Press Restart to restart the gateway working with the new parameters and press Continue to setup other parameters.

4.4.3 SYSLOG

Syslog is a standard method of centralizing various logs. You can use a syslog server to store your servers logs in a remote location for later perusal or long-term storage.

Click SYSLOG to configure



To send logs to the LOG server, you must configure the other servers from your network to send logs to that server.

Syslog Service setup

1. Click the enable item of **Syslog Server Service** to turn on syslog service.
2. Select the syslog server facility. The log facility allows you to send logs to different files in the syslog server.

Syslog Server Setup

3. Specify an server name to which all syslog messages will be sent.
4. Specify a UDP port number to which the syslog server is listening. The default value is 514. Make sure this is not blocked from your firewall.

Press Finish to finish the setup. The browser will prompt the configured parameters and check it before writing into NVRAM.

4.4.4 Time Sync

Time synchronization is an essential element for any business, which relies on the IT system. The reason for this is that these systems all have clock that is the source of timer for their filing or operations. Without time synchronization, these system's clocks vary and cause the failure of firewall packet filtering schedule processes, compromised security, or virtual server working in wrong schedule.

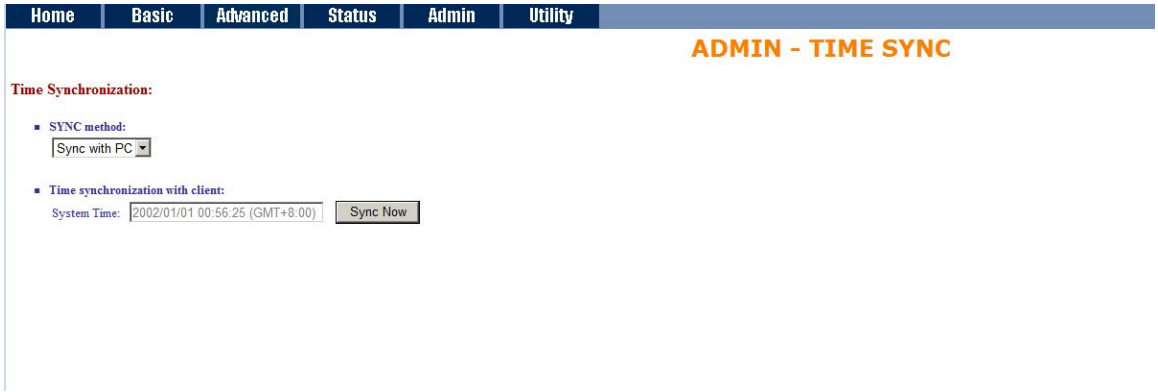
Click TIME SYNC.

Time synchronization has two methods:

Sync with PC	Synchronization with PC
SNTP v4.0.	Simple Network Time Protocol with Version 4

4.4.4.1 Synchronization with PC

For synchronization with PC, select Sync with PC. The router will synchronize the time with the connecting PC. The function can supported on both bridge and router mode.



4.4.4.2 SNTP v4.0

For using the SNTP, select SNTP v4.0.

SNTP is the acronym for Simple Network Time Protocol, which is an adaptation of the Network Time Protocol (NTP) used to synchronize computer clocks in the Internet. SNTP can be used when the ultimate performance of the full NTP implementation. The function only supported on router mode.

Service: Enable

Time Server 1, Time Server 2 and Time Server 3: All of the time server around the world can be used but suggest using the time server nearby to your country. You can set up maximum three time server on here.

Time Zone: Select the time difference between UTC(Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone from the drop-down list box.

Update Period: How many times the router can resynchronize to time server. The unit is second.

Press Finish to finish the setup. The browser will prompt the configured parameters and check it before writing into NVRAM.

.

4.5 Utility

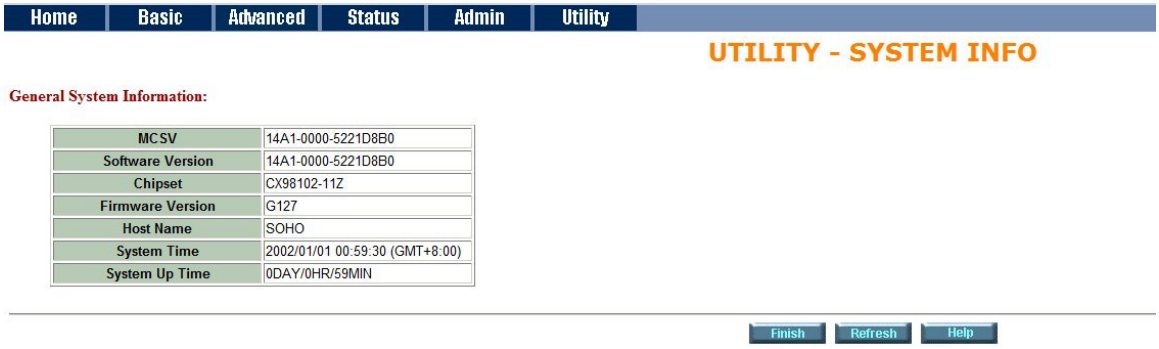
This section will describe the utility of the product including:

SYSTEM INFO	Show the system information
SYSLOG	Capturing log information
CONFIG TOOL	Load the factory default configuration, restore configuration and backup configuration
UPGRADE	Upgrade the firmware
LOGOUT	Logout the system
RESTART	Restart the router.

4.5.1 System Info

Click System Info to view the information.

The browser will prompt the system information.



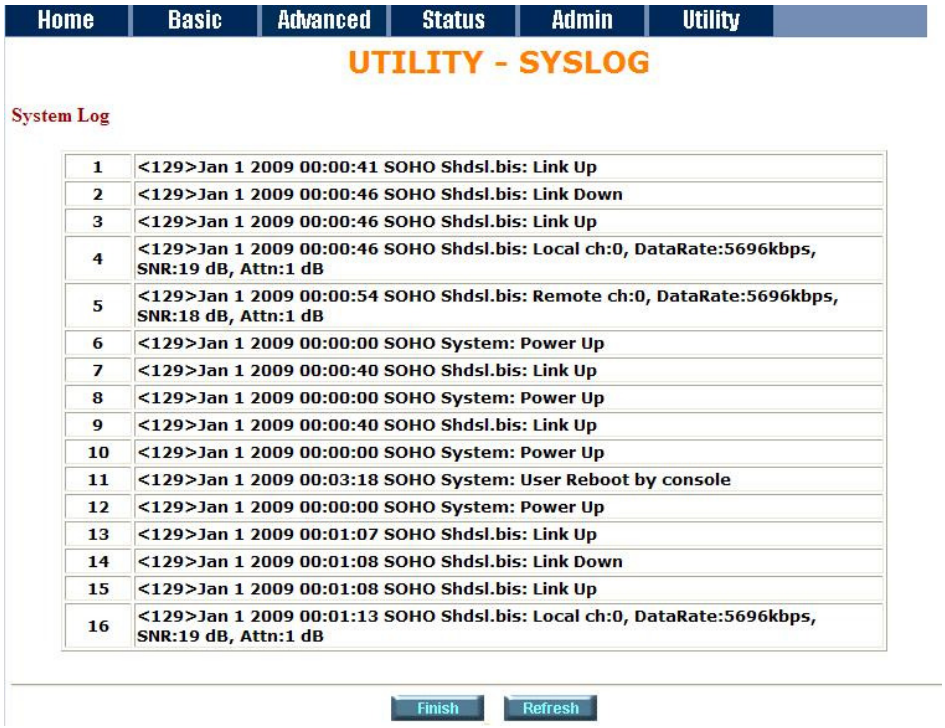
It will display general system information including: MCSV, software version, chipset, firmware version, Host Name, System Time and System Up Time.

MCSV: For internal identification purposes.
Software Version: This is the router's firmware version. Sometimes the technicians need it to troubleshoot problems.
Chipset: This is the SHDSL.bis chipset model name.
Firmware Version: This is the chipset's firmware version.
Host Name: This is the system name in BASIC Setup. It is for identification purposes.
System Time: This field displays the router's present date and time.
System Up Time: This is the total time that the router has been on.

4.5.2 SYSLOG

SHDSL.bis routers support detailed logging via Syslog function. The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event message. The router can generate a syslog message and send it to a syslog server.

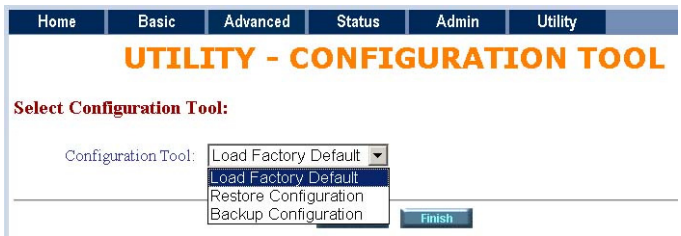
Press SYSLOG, it sends the syslog messages shown as follows:


Home
Basic
Advanced
Status
Admin
Utility
UTILITY - SYSLOG
System Log
1 <129>Jan 1 2009 00:00:41 SOHO Shdsl.bis: Link Up
2 <129>Jan 1 2009 00:00:46 SOHO Shdsl.bis: Link Down
3 <129>Jan 1 2009 00:00:46 SOHO Shdsl.bis: Link Up
4 <129>Jan 1 2009 00:00:46 SOHO Shdsl.bis: Local ch:0, DataRate:5696kbps, SNR:19 dB, Attn:1 dB
5 <129>Jan 1 2009 00:00:54 SOHO Shdsl.bis: Remote ch:0, DataRate:5696kbps, SNR:18 dB, Attn:1 dB
6 <129>Jan 1 2009 00:00:00 SOHO System: Power Up
7 <129>Jan 1 2009 00:00:40 SOHO Shdsl.bis: Link Up
8 <129>Jan 1 2009 00:00:00 SOHO System: Power Up
9 <129>Jan 1 2009 00:00:40 SOHO Shdsl.bis: Link Up
10 <129>Jan 1 2009 00:00:00 SOHO System: Power Up
11 <129>Jan 1 2009 00:03:18 SOHO System: User Reboot by console
12 <129>Jan 1 2009 00:00:00 SOHO System: Power Up
13 <129>Jan 1 2009 00:01:07 SOHO Shdsl.bis: Link Up
14 <129>Jan 1 2009 00:01:08 SOHO Shdsl.bis: Link Down
15 <129>Jan 1 2009 00:01:08 SOHO Shdsl.bis: Link Up
16 <129>Jan 1 2009 00:01:13 SOHO Shdsl.bis: Local ch:0, DataRate:5696kbps, SNR:19 dB, Attn:1 dB
Finish
Refresh

4.5.3 Config Tool

This configuration tool has three functions: load Factory Default, Restore Configuration, and Backup Configuration.

Press CONFIG TOOL.



Choose the function and then press Finish

4.5.3.1 Load Factory Default

Load Factory Default: It will load the factory default parameters to the router.

Note: This action will change all of the settings to factory default value. In other words, you will lose all the existing configured parameters.

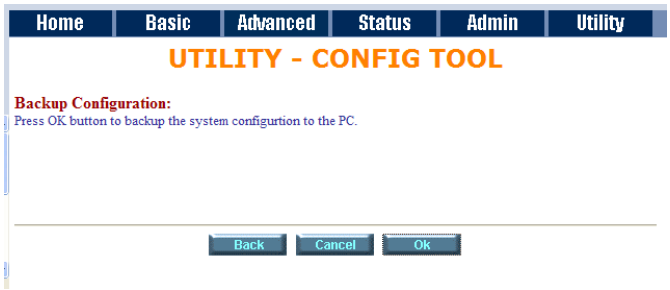
4.5.3.2 Restore Configuration

Sometimes the configuration could crush accidentally. It will help you to recover the backup configuration easily.

Click Finish after selecting Restore Configuration.
Browse the route of backup file then press Finish. Brower the location of restore file name or enter the name directly. Then press OK. The router will automatically restore the saved configuration.

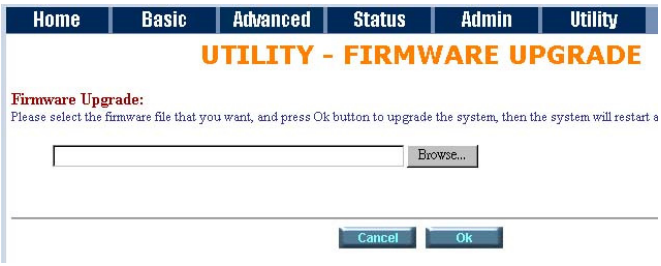
4.5.3.3 Backup Configuration

After completing the configuration of the router, please use this function to backup your router parameters in the PC. Select the Backup Configuration and then press Finish. Browse the location of backup file name or enter the name directly. Then press OK. The router will automatically backup the configuration. If you don't enter a file name, the system will use the default: *config1.log*



4.5.4 Upgrade

You can upgrade the router by using the upgrade function.
Press Upgrade in UTILITY.

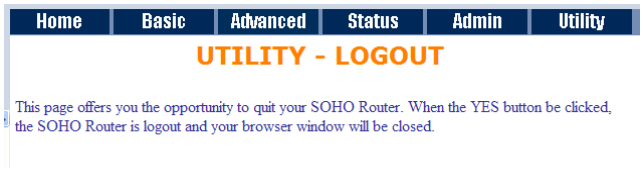


Select the firmware file name by clicking Browse on your PC or NB, and then press OK button to upgrade. The system will reboot automatically after finishing the firmware upgrade operation.

4.5.5 Logout

To logout the router, press LOGOUT in UTILITY.

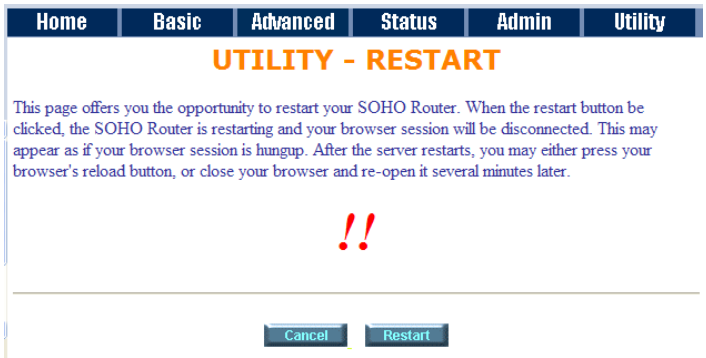
For logout system and close window, click the LOGOUT in UTILITY


Home
Basic
Advanced
Status
Admin
Utility
UTILITY - LOGOUT
This page offers you the opportunity to quit your SOHO Router. When the YES button be clicked,
the SOHO Router is logout and your browser window will be closed.

When click the Yes button, the Router will logout and browser window will be closed.

4.5.6 Restart

To restart the router, click the RESTART in UTILITY.

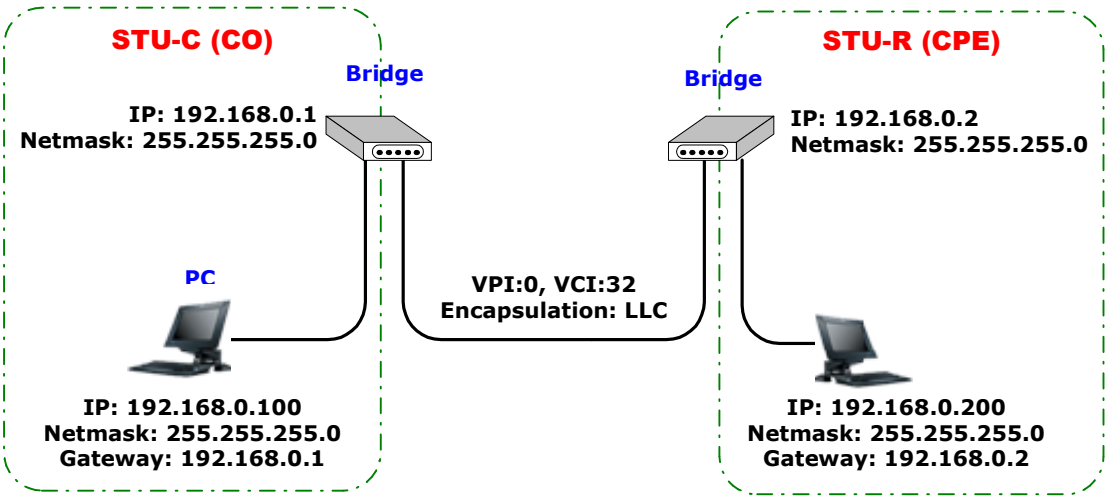

Home
Basic
Advanced
Status
Admin
Utility
UTILITY - RESTART
This page offers you the opportunity to restart your SOHO Router. When the restart button be clicked, the SOHO Router is restarting and your browser session will be disconnected. This may appear as if your browser session is hungup. After the server restarts, you may either press your browser's reload button, or close your browser and re-open it several minutes later.
!!
Cancel
Restart

Press Restart to reboot the router.

When the restart button was clicked, the router will restart and the browser session will be disconnected. This may appear as if your browser session is hung up. After the router restarts, you may either click the browser's reload button or close the browser and re-open it later.

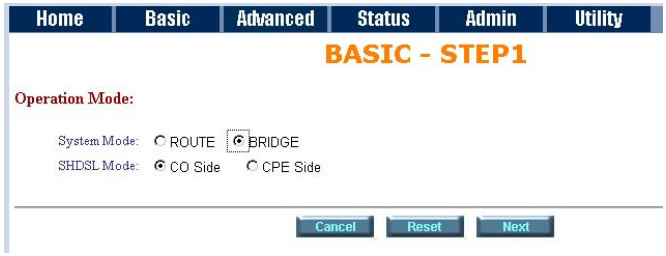
4.6 Example

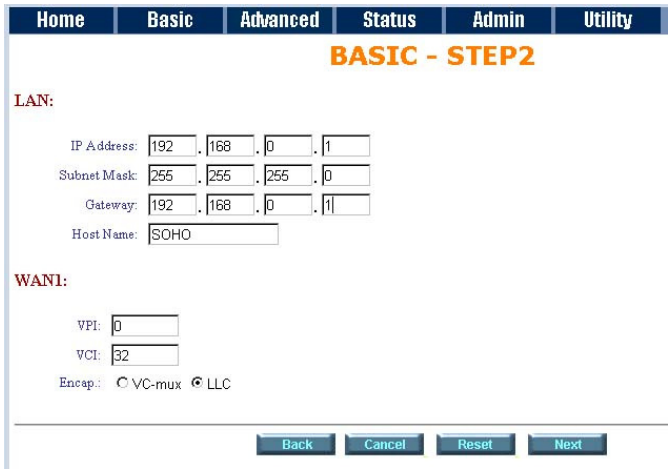
4.6.1 LAN-to-LAN connection with bridge Mode



4.6.1.1 CO side

Click Bridge and CO Side to setup Bridging mode of the Router and then click Next.





Enter **LAN** Parameters
IP: 192.168.0.1
Subnet Mask: 255.255.255.0
Gateway: 192.168.0.1

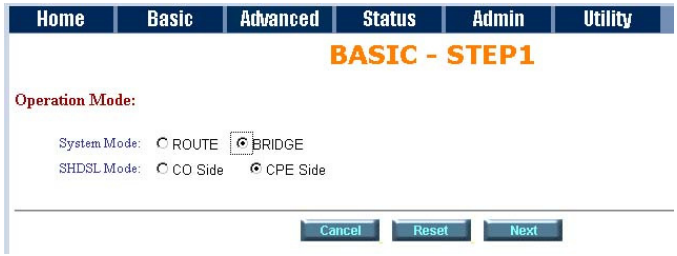
Host Name: SOHO

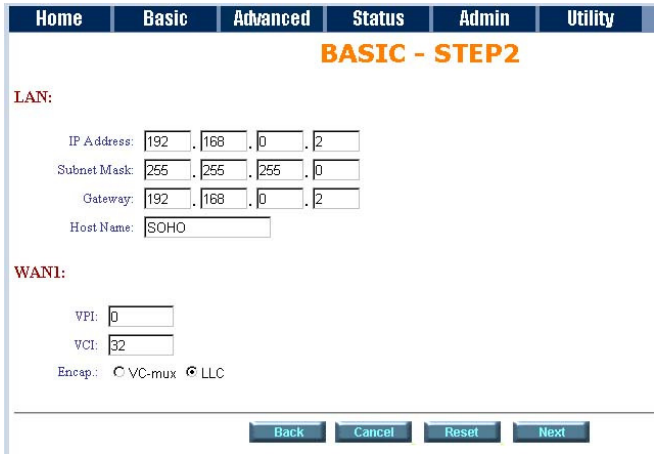
Enter **WAN1** Parameters
VPI: 0
VCI: 32
Click LLC
Click Next

The screen will prompt the new configured parameters. Check the parameters and Click Restart
The router will reboot with the new setting.

4.6.1.2 CPE Side

Click Bridge and CPE Side to setup Bridge mode of the Router and then click Next.



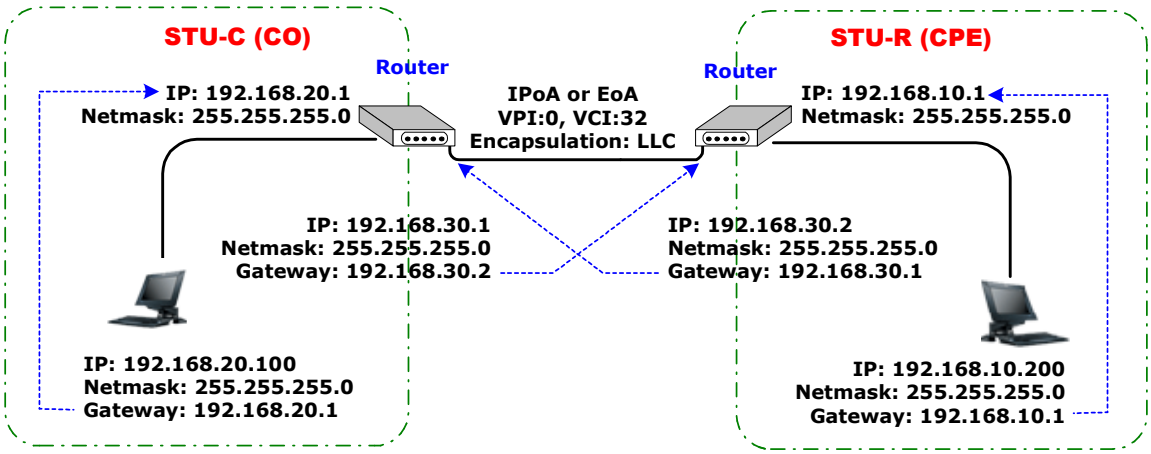


Enter **LAN** Parameters
IP: 192.168.0.2
Subnet Mask: 255.255.255.0
Gateway: 192.168.0.2
Host Name: SOHO

Enter **WAN1** Parameters
VPI: 0
VCI: 32
Click LLC
Click Next

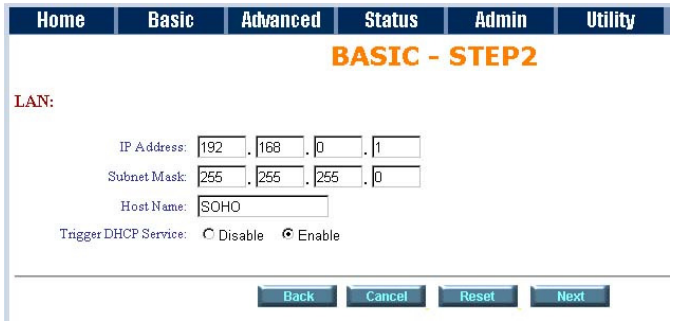
The screen will prompt the new configured parameters. Check the parameters and Click Restart
The router will reboot with the new setting.

4.6.2 LAN to LAN connection with routing mode

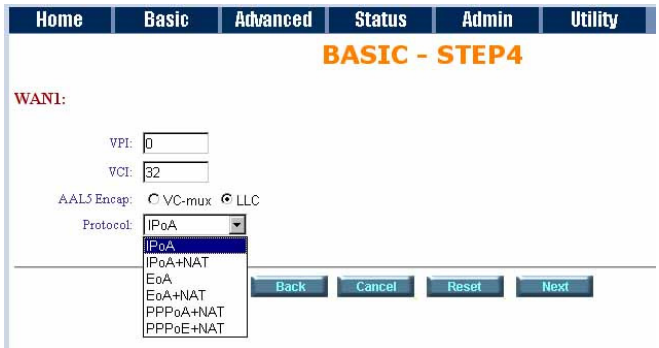


4.6.2.1 CO Side

Click ROUTE and CO Side to setup Routing mode of the Router and then click Next



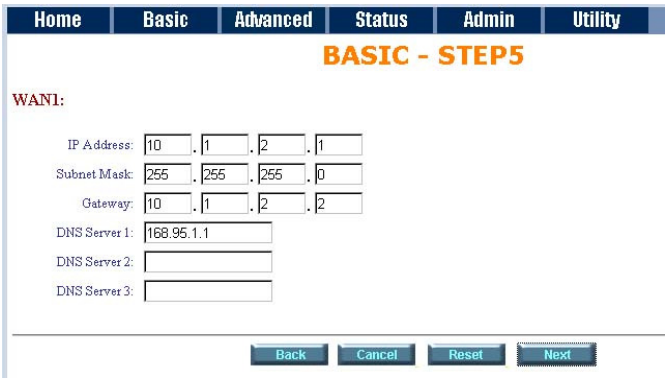
Type **LAN** parameters:
IP Address: 192.168.20.1
Subnet Mask: 255.255.255.0
Host Name: SOHO
DHCP Service: Disable or Enable
For more **DHCP** service, review the chapter on DHCP Service



Type the **WAN1** Parameters;
VPI: 0

VCI: 32
AAL5 Encap: LLC
Protocol: IPoA , EoA , IPoA + NAT or EoA + NAT
Note: The Protocol used in CO and CPE have to be the same.
Click Next to setup the IP parameters.

For more understanding about **NAT,** review the chapter of NAT/DMZ .



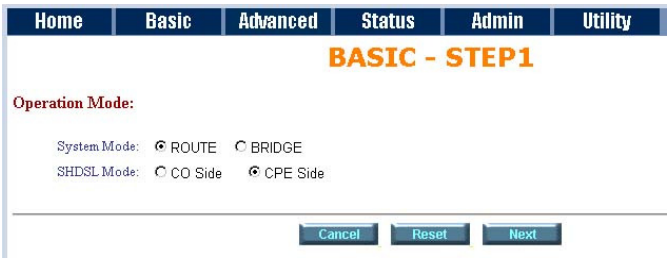
IP Address: 192.168.20.1
Subnet Mask: 255.255.255.0
Gateway: 192.169.30.2
Click Next

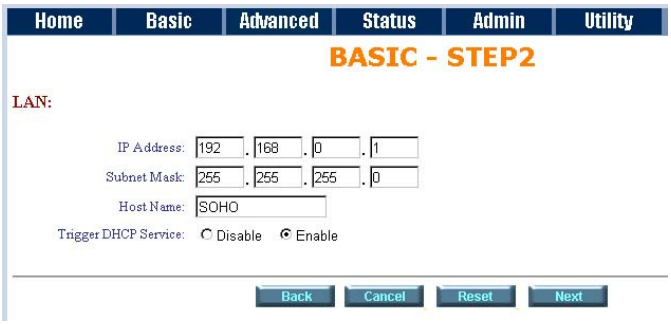
The screen will prompt the parameters that will be written in NVRAM. Check the parameters before writing in NVRAM.

Press Restart to restart the router working with new parameters or press continue to setup another parameter.

4.6.2.2 CPE side

Click ROUTE and CPE Side then press Next.





Type LAN parameters:

IP Address: 192.168.10.1

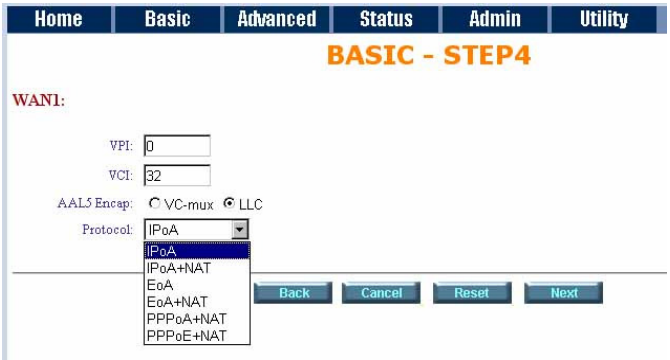
Subnet Mask: 255.255.255.0

Host Name: SOHO

DHCP Service: Disable or Enable

For more **DHCP** service, review the chapter of DHCP Service.

Type the WAN1 Parameters:



VPI: 0

VCI: 32

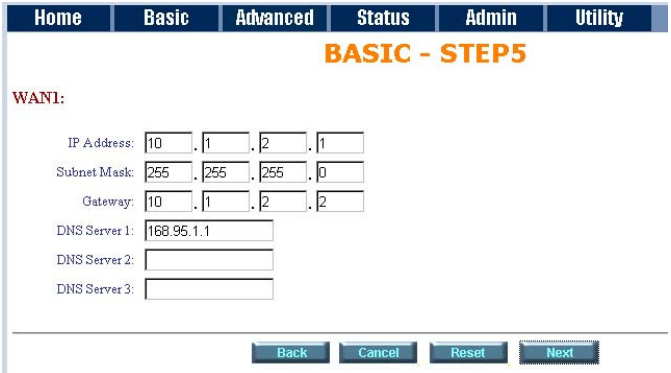
AAL5 Encap: LLC

Protocol: IPoA , EoA , IPoA + NAT or EoA + NAT

Note: The Protocols used in CO and CPE have to be the same.

Click Next to setup the IP parameters.

For more understanding about **NAT**, review the chapter of NAT/DMZ.



IP Address: 192.168.30.2

Subnet mask: 255.255.255.0

Gateway: 192.169.30.1

Click Next

The screen will prompt the parameters that will be written in NVRAM. Check the parameters before writing in NVRAM.

Press Restart to restart the router working with new parameters or press continue to setup another parameter.

5 Configuration via Serial Console or Telnet with Manu Driven Interface

In this section, the detail of menu-driven user interface will be described as follows.

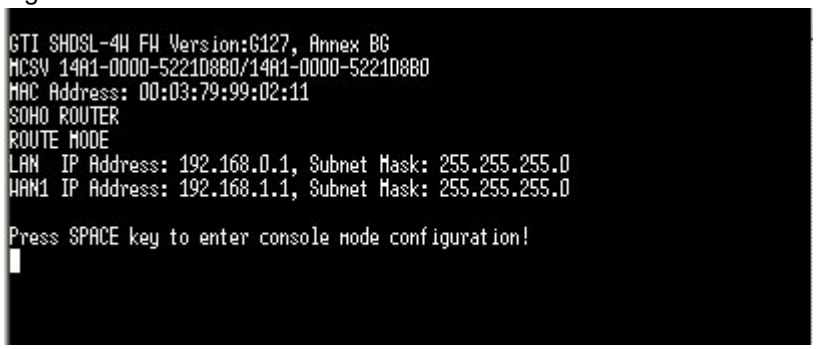
5.1 Introduction

5.1.1 Serial Console

Check the connectivity of the RS-232 cable. Connect the male 9-pin end of console port of the router and connect the female end to a serial port of your computer.
Start your terminal access program by VT100 terminal emulation with the following parameters:

Parameter	Value
Baudrate	9600bps
Data Bits	8
Parity Check	No
Stop Bits	1
Flow-control	No

Press the SPACE key until the login screen appears. When you see the login screen, you can logon to Router.


GTI SHDSL-4W FW Version:G127, Annex BG
MCSV 14A1-0000-5221D8BD/14A1-0000-5221D8BD
MAC Address: 00:03:79:99:02:11
SOHO ROUTER
ROUTE MODE
LAN IP Address: 192.168.0.1, Subnet Mask: 255.255.255.0
WAN1 IP Address: 192.168.1.1, Subnet Mask: 255.255.255.0
Press SPACE key to enter console mode configuration!

Note: Only SPACE key invoke the login prompt. Pressing other keys does not work.

```
User: admin
Password: *****
```

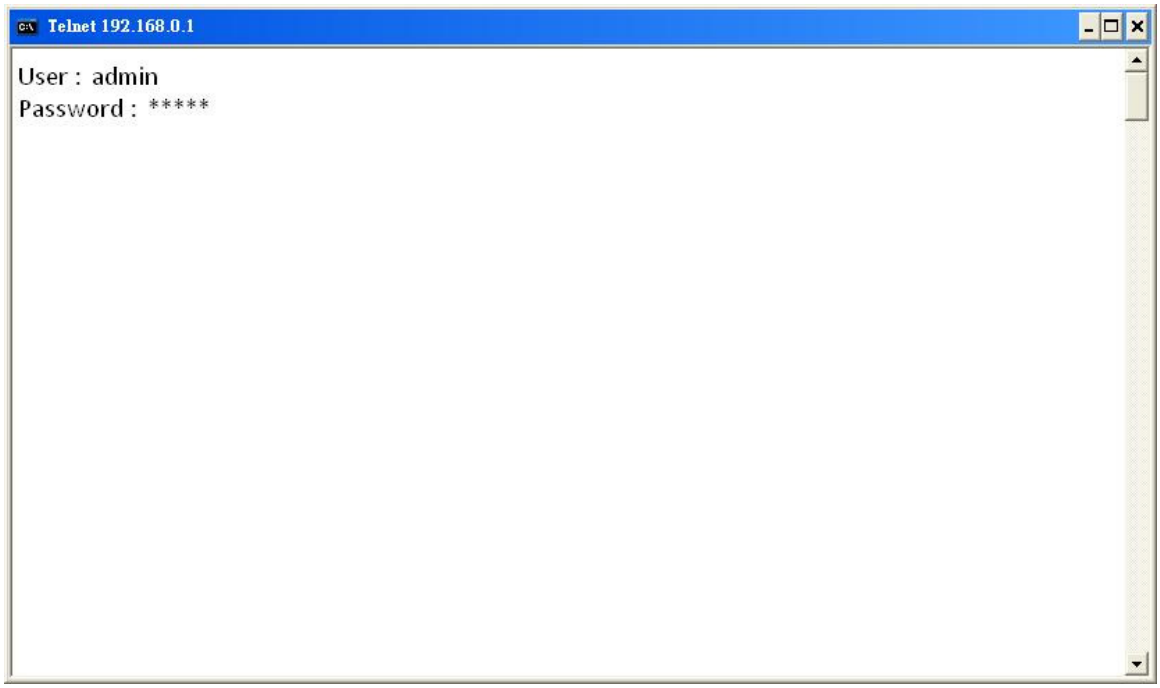
Note: The factory default **User** and **Password** are “admin” both.

5.1.2 Telnet

Make sure the correct Ethernet cable connected the LAN port of your computer to this Router. The LAN LNK LED indicator on the front panel shall light if a correct cable is used. Starting your Telnet client with VT100 terminal emulation and connecting to the management IP of Router, wait for the login prompt appears. Input User and Password after login screen pop up,

```
User: admin
Password: *****
```

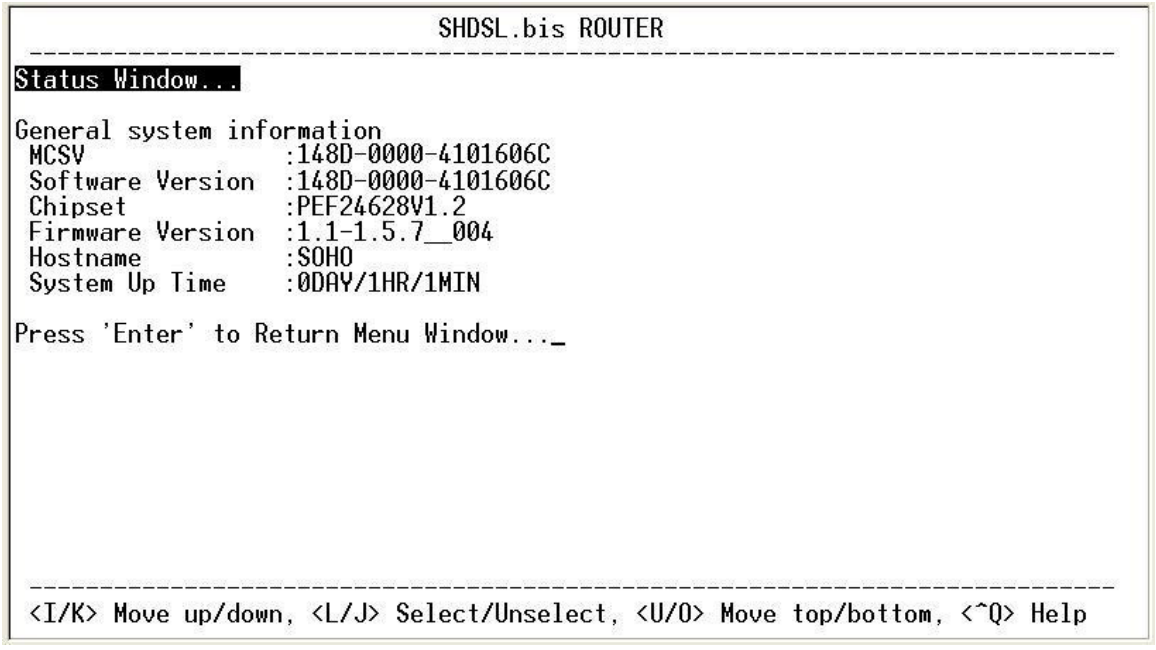
Note: The default IP address is 192.168.0.1.



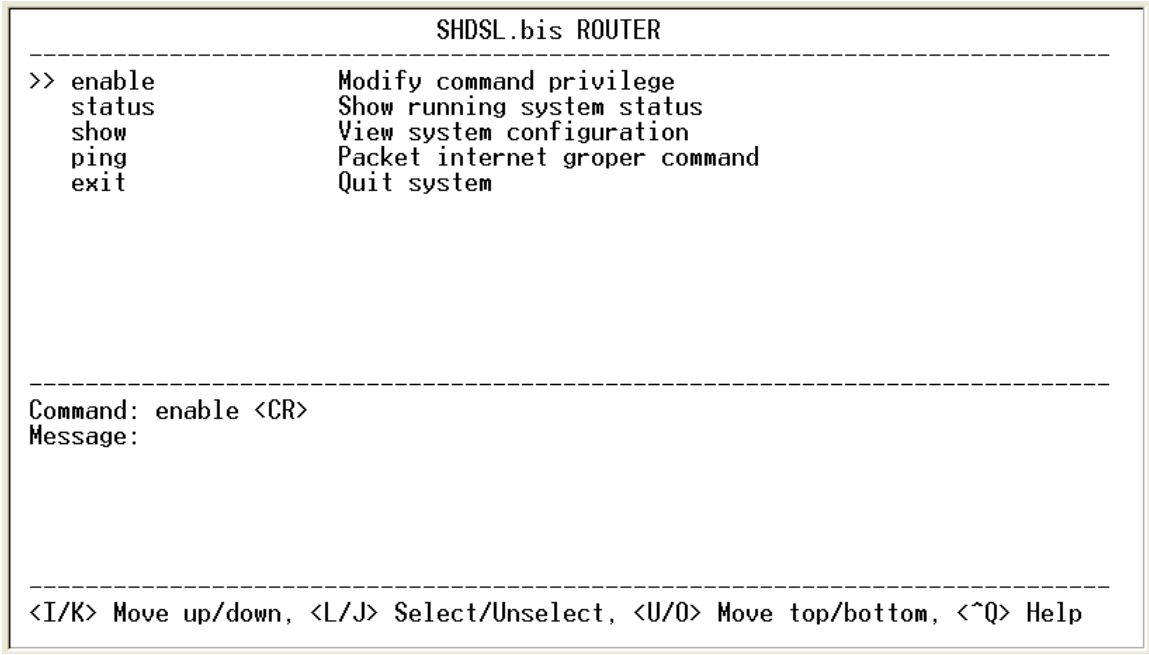
5.1.3 Operation Interface

For serial console and Telnet management, the Router implements two operational interfaces: Command Line Interface (CLI) and menu driven interface. The CLI mode provides users a simple interface, which is better for working with script file. The menu driven interface is a user-friendly interface to general operations. The command syntax for CLI is the same as that of the menu driven interface. The only difference is that the menu driven interface shows you all of available commands for you to select. You don't need to remember the command syntax and save your time on typing the whole command line.

The following figure gives you an example of the menu driven interface. In the menu, you scroll up/down by pressing key **I** / **K**, select one command by key **L**, and go back to a higher level of menu by key **J**.
For example, to show the system information, just logon to the Router, move down the cursor by pressing key **K** twice and select "show" command by key **L**, you shall see a submenu and select "system" command in this submenu, then the system will show you the general information.



5.1.4 Window structure



From top to bottom, the window is divided into four parts:

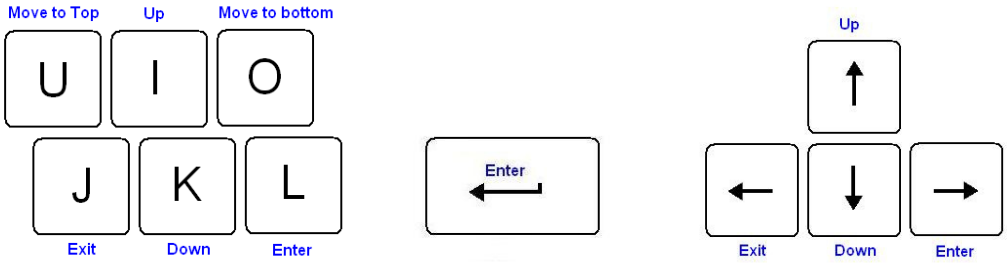
1. **Product name**: "SHDSL.bis ROUTER"
2. **Menu field**: Menu tree prompts on this field. Symbol "**>>**" indicates the cursor place.
3. **Configuring field**: You will configure the parameters in this field. **< parameters >** indicates the parameters you can choose and **< more…>** indicates that there is submenu in the title.
4. Operation command for help

The following table shows the parameters in the brackets.

Command	Description
<ip>	An item enclosed in brackets is required. If the item is shown in lower case bold, it represents an object with special format. For example, **<ip>** may be **192.168.0.3**.
<Route|Bridge>	Two or more items enclosed in brackets and separated by vertical bars means that you must choose exactly one of the items. If the item is shown in lower case bold with leading capital letter, it is a command parameter. For example, **Route** is a command parameter in **<Route|Bridge>**.
[1~1999]	An item enclosed in brackets is optional.
[1~65534|-t]	Two or more items enclosed in brackets and separated by vertical bars means that you can choose one or none of the items.

5.1.5 Menu Driven Interface Commands

Before changing the configuration, familiarize yourself with the operations list in the following table. The operation list will be shown on the window.



```
ERROR: stackunderflow
OFFENDING COMMAND: ~

STACK:
```